CRIMINALÍSTICA COMPUTACIONAL: MODELO PARA LA ESTRUCTURACIÓN DE EVIDENCIAS

Jennifer Vanessa Cárdenas Criollo

Pavel Enrique Ramírez Castillo

UNIVERSIDAD LIBRE

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE SISTEMAS

BOGOTÁ DC

Marzo 02 de 2017

CRIMINALÍSTICA COMPUTACIONAL: MODELO PARA LA ESTRUCTURACIÓN DE EVIDENCIAS

Jennifer Vanesa Cárdenas Criollo
Pavel Enrique Ramírez Castillo

PROYECTO DE GRADO PRESENTADO COMO REQUISITO PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

DIRECTOR: EDUARDO TRIANA M.
INGENIERO DE SISTEMAS

UNIVERSIDAD LIBRE
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
BOGOTÁ DC
Marzo 02 de 2017

NOTA DE ACEPTACION

_____

_____

_____

_____

_____

Ing. Mauricio Alonso Moncada

Director Programa

_____

Ing. Eduardo Triana M

Presidente de Jurado

_____

Ing. Fabián Blanco Garrido

Jurado Calificador

_____

Ing. Fredys Simanca H

Jurado Calificador

BOGOTA, MARZO 02 DE 2017

DEDICATORIA

Dedico esta tesis a Dios por haberme permitido llegar hasta este punto, haberme dado salud para cumplir mis objetivos, por guiarme por el buen camino y darme fuerzas para no desmayar ante los problemas y dificultades que se presentaban.

Jennifer Vanesa Cárdenas Criollo.

DEDICATORIA

Primero a ti Dios por bendecirme para llegar hasta donde he llegado, porque hiciste realidad este sueño anhelado. A mi madre Luz Marina Castillo Cardenas, por ser una mujer hermosa, excepcional, a mi padre Enrique Ramirez Cadena que siempre está conmigo y siempre tienes una palabra de apoyo con mucho amor en momentos complejos de mi vida, a mi tia Ludivia Ramirez Cadena, por tu apoyo incondicional, a mi hermana Zulkerine Ramirez Cadena y familia y a mi hijo Nicolás Ramirez Neira que a pesar de la distancia siento que estás conmigo siempre, aunque nos faltan muchas cosas por vivir.

Pavel Enrique Ramírez Castillo

AGRADECIMIENTOS

Agradezco a mis padres Mauricio Cardenas y Bellanira Criollo, por apoyarme en todo momento, por sus consejos y sus valores, por la ayuda que me brindaron en los momentos difíciles, me han dado todo lo que soy como persona; agradezco a mi familia, mis compañeros y mis profesores a quienes sin su ayuda no hubiera podido culminar mis estudios. Muchas gracias a todos por su apoyo incondicional. Quiero darle un especial reconocimiento al Ing. Eduardo Triana por toda su ayuda y las sugerencias recibidas durante la elaboración de esta tesis. A todos y cada uno de ustedes gracias por ayudarme a cumplir esta meta.

Jennifer Vanesa Cárdenas Criollo.

AGRADECIMIENTOS

A la Universidad Libre de Colombia por darme la oportunidad de estudiar y ser un profesional, a mi director de tesis, el ingeniero Eduardo Triana Moyano por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia, su paciencia y su motivación ha logrado en nosotros que podamos terminar nuestros estudios con éxito.

También me gustaría agradecer a mis profesores durante toda mi carrera profesional porque todos han aportado con un granito de arena a mi formación.

A mi jefe de trabajo el Dr. German Dario Amortegui Rodriguez, quien es como un padre para mí, los cuales me ha motivado durante mi formación profesional.

A toda mi familia por siempre estar conmigo en todos los momentos de mi vida.

Son muchas las personas que han formado parte de mi vida profesional y emocional a las que quisiera agradecerles su amistad, consejos, apoyo, ánimo y compañía. Algunas están aquí conmigo y otras en mis recuerdos y en mi corazón, sin importar en donde estén quiero darles las gracias por formar parte de mí, por todo lo que me han brindado y por todas sus bendiciones.

Pavel Enrique Ramírez Castillo

TABLA DE CONTENIDO

PAGINA

LISTADO DE FIGURAS

PAGINA

LISTADO DE ANEXOS

PAGINA

GLOSARIO

ALERTA: Acción logística que genera un despliegue operacional de las políticas y servicios de seguridad con el fin de restringir o anular la estructuración invasora de código malicioso, Ramsonware, Spam o anzuelos (Phishing).

AMENAZA: Termino que registra la intencionalidad para atentar contra la seguridad de la información, producto de la existencia de vulnerabilidades en el sistema transaccional.

ATAQUE: Operación causada por los llamados piratas de la información al explotar una vulnerabilidad, con el fin de estropear o modificar valores informáticos o congelar una arquitectura de cómputo.

AUDITABILIDAD: Principio de la seguridad informática, orientado al registro y monitoreo de la función de utilización de los recursos configurados y asignados según perfil de catalogación en un sistema Teleinformatico.

AUTENTICACION: Actividad desarrollada por el sistema, para validar el perfil de operación que se asigna a un usuario y habilitar su interacción.

CIBERTERRORISMO: Uso de entidades e infraestructuras logísticas informáticas para generar daños en infraestructuras computacionales, quebrantando los modelos de ciberseguridad y ciberdefensa, con el fin de generar destrucciones que se tipifican legalmente como delitos según legislación universal.

DEGAUSSER: Actividad que mediante la desmagnetizacion del espectro lógico de mapeo impide la recuperación de la información almacenada al eliminar la huella de lectura o visualización operacional

DELITO INFORMATICO: Acción dolosa que modifica o destruye un valor informático, cuyo efecto es penado según normatividad jurídica existente a la luz del estado de derecho con el fin de juzgar al imputado.

DENEGACION DEL SERVICIO: Ataque a una red o sistema de computadoras que genera que un servicio o recurso sea inaccesible a los usuarios que son legítimos.

ECOSISTEMA DIGITAL: Unidad de referenciación operacional que define en el ciberespacio las operaciones de intercambio transaccional de contenidos, procesos y servicios, al operar arquitecturas computacionales cuya configuración se orienta al flujo de valores informáticos sobre Internet.

ESTEGANOGRAFIA: Parte de la criptologia donde se aplican y estudian las técnicas que permiten el ocultamiento de mensajes u objetos.

EVIDENCIA: Entidad valorada jurídicamente por su grado de certeza, como unidad del acervo probatorio en la consideración de un delito informático.

FIREWALL: Dispositivo que bloquea el acceso no autorizado a un sistema Teleinformatico, limitando el flujo transaccional, descifrando o cifrando los valores que fluyen, con el fin de reducir las acciones configuradas por un vector de ataque.

GESTION DE LOGS: Actividad orientada a controlar, modificar y actualizar los registros que almacena la bitácora operacional del sistema, para validar la significancia e integridad durante la interacción del usuario según perfil configurado

HFSX: Sistema de archivos que modifica y actualiza la estructura convencional de Apple HFS, para extender su usabilidad a 256 bytes, 32 bits y manejo pleno de UNICODE

ICCID (Integradted circuit card identifier): Identificador de la tarjeta, almacenado en la SIM del teléfono móvil, que señala el país, red y circuito de enlace o distribuidor.

INTRUSO: Sujeto que invade la operación del sistema, con el fin de modificar o destruir su integridad.

JAILBREAK: Operación que permite acceder al sistema operativo por escalamiento de privilegios.

MASTER BOOT RECORD (MBR): Registro que condiciona el proceso de acceso a un disco, al configurar el esquema de control de recorrido.

MECANISMO DE SEGURIDAD: Técnica que permite implementar servicios asociados con la especificación de controles.

MEMORIA FLASH: Memoria EEPROM, que permite acceder para leer o escribir múltiples posiciones de memoria, gracias a los atributos funcionales de la tecnología del estado sólido.

PERFIL: Especificación funcional que cataloga la operación e interacción de un usuario con el sistema.

PIN: Número de identificación personal utilizado en ciertos sistemas, como el teléfono móvil o el cajero automático, para identificarse y obtener acceso al sistema

PLATAFORMA: Unidad de catalogación y referenciación lógica que el usuario opera en el entorno Teleinformatico y computacional.

PRACTICA: Estructuracion aplicativa de un servicio de seguridad o de catalogación jurídica de una evidencia

PROVEEDOR: Referente que libera servicios o procesos en el ambiente de proceso computacional

PROXY: Unidad que intercepta eventos y transacciones en la red con el fin de garantizar la confiabilidad e integridad de la operación realizada

PUK: Código de 8 bytes que desbloquea la tarjeta SIM, al detectar información equivoca

RFC 2828: Vademécum tecnológico de especificación normativa de la seguridad según modelo OSI

SERVICIO DE SEGURIDAD: Unidad de especificación y estructuración lógica que garantiza al usuario el trabajo limpio y plena confiabilidad en la red.

SET (Secure Electronic Transaction): Protocolo que garantiza la realización segura de una transacción en el ámbito de los negocios electrónicos.

TLS (Transport Layer Security): Protocolos criptográficos que proporcionan comunicaciones seguras por una red.

TRAZABILIDAD: Nivel analítico de especificación de la funcionalidad y significancia de una operación, que permite evaluar el impacto de modificación causado

TRIM: Comando que en la tecnología del estado sólido, habilita al sistemas para valorar la disponibilidad de espacio configurado, habilitando la no recuperación lógica y física de valores almacenados.

X509: Es un estándar UIT-T para infraestructuras de claves públicas (en inglés, Public Key Infraestructura o PKI), que señala los estándares para certificados de claves públicas junto con el algoritmo de validación a implementar.

X800: Especificación normativa que define la arquitectura de seguridad, según consideraciones de interconexión OSI/ISO.

RESUMEN

El incremento progresivo de ataques a los sistemas Teleinformáticos, por parte de los intrusos, quienes como piratas y bucaneros de la información, estropean las arquitectura computacionales y destruyen o modifican los valores informáticos, haciendo que la función de utilidad en la organización cibernética se minimice y por ende la catalogación del PIB, al interior de la llamada economía naranja se reduzca, ha desafiado y motivado a los expertos en el tratamiento e instrumentación de la seguridad informática, para que se ocupen del diseño, configuración y estructuración de esquemas lógicos e integrales, que faciliten la selección y estructuración de evidencias, que permitan la formalización legal ante los estrados judiciales del delito informático cometido producto del ataque realizado a un ecosistema digital declarado como objetivo.

Si bien se cuenta en la actualidad con poderosas herramientas tanto a nivel hardware como software para apoyar la función del perito en informática forense, que enfrenta los desafíos formulados por la criminalística digital, se hace preciso que el talento Ingenieril con su lógica, creatividad e innovación, valore el potencial de su pensamiento convergente y divergente y proyecte la estructuración de modelos operacionales que regenten el proceso de acopio, clasificación y formulación de indicios o evidencias, con las cuales se podrá identificar seguir y presentar ante el estrado judicial al intruso o responsable del delito cometido, según legislación existente , para atender lo pertinente a los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

PALABRAS CLAVES: Cadena de Custodia; Delito Informático; Ecosistema Digital, Evidencia; Informática forense.

ABSTRACT

The progressive increase of attacks to systems telematics, by the intruders, who as pirates and Buccaneers of the information, spoil the computer architecture and destroy or modify computer values, causing the utility function in the Cyber organization is minimized and thus slows the cataloging of GDP, to the interior of the special stage of the humanity: **Orange economy** He has challenged and motivated experts in treatment and implementation of computer security, so they take up the design, configuration and structuring of integrals, that facilitate the selection and structuring of evidence, allowing the legal registration before judicial podiums of the crime computer product of the attack to a digital ecosystem declared objective and logical schemas.

While is has currently with powerful tools both to level hardware as software for support the function of the expert in computer forensic, that faces them challenges formulated by the Criminology digital, is makes precise that the talent engineering with its logical, creativity e innovation, values the potential of his thought convergent and divergent and project it structuring of models operational that run the process of gathering , classification and formulation of evidence or evidence, with which is may identify follow and present before the podium judicial to the intruder or responsible of the crime committed, according to legislation existing, for meet it relevant to them attacks against the confidentiality, the integrity and the availability of them data and of them systems computer.

KEYWORDS: Chain of custody; Computer Criminology; Computer Forensics; Digital ecosystem, Evidence.

INTRODUCCIÓN

La información en la economía naranja o del conocimiento, se valora como el activo fijo más preciado de la organización, razón por la cual el incremento progresivo de los ataques y amenazas estructurados por los Hackers, Crackers, Script Kiddies, Phreaker, Newbie, Lammer, o Wanna Be, hace que los expertos o peritos en informática forense se ocupen de elaborar estrategias orientadas a minimizar, eliminar, identificar, seguir y asegurar la judicialización de estos intrusos; los profesionales en seguridad informática, estudian los alcances del Ciberterrorismo, profundizan en las técnicas de la esteganografia en video, se preocupan por evaluar la potencialidad de la tecnología en ambientes virtuales y detallan los esquemas operacionales de la tecnología del estado sólido, para definir marcos referenciales y modelos de operación, que interactúan con el nuevo bien jurídico tutelado por la legislación Colombiana.

El ecosistema tecnológico posee procesos, infraestructura y sistemas de información, definidos sobre una plataforma y un proveedor, manifestados en el entorno computacional nominal o dentro de la computación en la nube (Cloud Computing), el seguimiento de rastros, el acopio de indicios o evidencias, la definición de la cadena de custodia y la presentación formal ante el escenario judicial, exigen al perito forense digital, el valorar con objetividad el ciclo de vida de la evidencia, para determinar, asociar y tipificar el delito cometido: Acceso abusivo a un sistema informático, Obstaculización ilegítima de sistema informático, Interceptación de datos informáticos, Uso de software malicioso o Suplantación de sitios web, teniendo entonces que recurrir a un modelo, cuya funcionalidad sistémica proporcione los reguladores y especificadores logísticos que garantizaran cumplir con solvencia las consideraciones establecidas para el manejo de pruebas electrónicas por parte de la fiscalía designada para actuar sobre el delito informático cometido, acorde con la ley 1273.

El desarrollo de este trabajo, se estructura en tres apartados o referenciales descriptivos, en el primero se presenta el marco operacional de desarrollo, contextualizando la pregunta de estudio y definiendo la carta de navegación metodológica, luego se detalla el andamiaje infraestructural teórico que sustentara la construcción del entregable, considerando aspectos fundamentales de la seguridad

digital, los sistemas de comunicación de computadores y las bases de operación de la informática forense .

1. MARCO REFERENCIAL DE DESARROLLO

En este capítulo se presenta el marco sistémico de contextualización, que facilite al lector interesado, interpretar con significancia el trabajo realizado, al permitirle conocer, su estructura operacional, valorar la integridad de los objetivos formulados, categorizar los resultados esperados e identificar la pertinencia de la metodología seleccionada, dentro del eje analítico y relacional que determina la investigación tecnológica aplicada para definir la normativa que coadyuvará a construir con calidad un producto ingenieril que impactara por su efectividad y usabilidad las esferas de la sociedad, la producción y el pensamiento; aspectos que se tratan a continuación:

1.1. IDENTIFICACIÓN DEL PROYECTO

Criminalística Computacional: Modelo para estructuración de evidencias

1.2. PLANTEAMIENTO SISTÉMICO DEL PROBLEMA

1.2.1. DESCRIPCIÓN DEL PROBLEMA

La criminalista computacional que registra el accionar de los Ciberdelincuentes[1], presento en el año 2015, según informe de seguridad para Colombia pérdidas por 1500 millones de pesos; la aplicación de las sanciones contempladas por la ley 1273. Han permitido a los jueces de la republica promulgar las soluciones pertinentes; no obstante la existencia de procesos regulatorios legales adecuados, algunos casos no pueden resolverse al carecer de normas procedimentales que defina la interacción de la investigación forense con el tratamiento de evidencias y el análisis forense dentro de los ecosistemas tecnológicos en donde se registra la acción de los enemigos de la información, producto de la no operación y direccionamiento de un modelo que facilite la criminalística digital y el tratamiento formal de la evidencia.

[1]Termino que referencia al conjunto de personas que actúan como enemigos de la información en la red y ocasionan con su accionar delitos tipificados en el código penal, al registrar consecuencias gravosas sobre el agente afectado. http://www.seguridadpc.net/conceptos/los-ciberdelincuentes.html.

1.2.2. FORMULACIÓN DEL PROBLEMA

¿Cómo abordar el análisis forense y el tratamiento pericial al estudiar el impacto fenomenológico en un ecosistema[2] un delito informático?

1.3. PRESENTACIÓN DE OBJETIVOS

1.3.1. OBJETIVO GENERAL

Construir el modelo funcional que sustentara la estructuración de evidencia dentro del proceso pericial definido por la criminalística computacional.

1.3.2. OBJETIVOS ESPECÍFICO

- Identificar y dimensionar los procesos lógicos del Ciberterrorismo y la Criminalística digital.
- Evaluar la integridad operacional del ecosistema digital, donde se presenta el delito informático.
- Conformar la base de acción recurrente para el proceso de acopio de evidencias, como valoradoras de las pruebas informáticas dentro del proceso pericial.

1.4. JUSTIFICACIÓN

El crecimiento de ataques por parte de los enemigos de la información que inquietan a la organización hiperconectada, permite que la ingeniería de sistemas, se ocupe de la construcción de soluciones orientadas a valorar y soportar los procesos pertinentes al escenario de la informática forense y la criminalística computacional; específicamente el interior del programa de ingeniería de sistemas de la Universidad Libre de Colombia, el desarrollo de la línea electiva de seguridad informática, demanda el soporte de instrumentos, documentos y referentes de acción pedagógica, que permitan la consolidación de su impacto en la comunidad estudiantil.

[2] Entidad cuya logística funcional integra sincrónicamente valoradores tecnológicos, referente informáticos y operadores que transforman las transacciones computacionales que operan sobre internet, en valores informáticos gracias a los servicios y ejes nativos definidos para construir un campo de acción decisional.
http://marketingenredesociales.com/que-es-y-para-que-sirve-el-ecosistema-digital-para-mi-pyme.html/

1.5. ALCANCE

El contenido de este trabajo, permitirá identificar las técnicas aplicadas por el intruso, producto de las consideraciones fundamentales de las infraestructuras de ciberseguridad[3] y ciberdefensa[4], y del apropiado manejo de la audibilidad y la trazabilidad, pudiéndose comprender la funcionalidad y transparencia de los procedimientos requeridos para realizar la investigación forense que requiere la dilucidación del delito informático cometido.

1.6. ESCENARIO DESCRIPTIVO INVESTIGATIVO

Este numeral registra, el marco descriptivo investigativo, las fases de la metodología definida como referencia básica de construcción junto con el eje de visualización grafico asociado con los tiempos programados para desarrollar las actividades trazadas.

1.6.1. TIPO DE INVESTIGACIÓN

El desarrollo y construcción de la solución, se sustenta en los fundamentos teóricos y principios normativos de la investigación tecnológica aplicada.

1.6.2. METODOLOGÍA OPERACIONAL

El desarrollo de un proyecto de base tecnológica, que involucra el análisis y tratamiento epistemológico de su fundamentación teórica y la correlación funcional de los núcleos que definen sus entradas, patrones de proceso y conjunto de variables de salida, demanda del seguimiento de las fases contempladas convencionalmente por el ciclo de vida, dada su especificidad, nivel de secuencialidad, sincronismo y coherencia formal, estas fases son referenciadas a continuación:

---

[3] Conjunto estructural cuya logística funcional establece las políticas y servicios que definen un escudo de protección para contrarrestar operaciones de la guerra electrónica y el Ciberterrorismo.
https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

[4] Plataforma logística que denota las acciones procedimentales que detectan, rastrean y eliminan los vectores de ataque configurados por los hackers o piratas de la información, como respuesta efectiva a los mecanismo catalogados por el gobierno o la organización inteligente
https://www.mindefensa.gov.co/irj/go/km/docs/Mindefensa/Documentos/descargas/estudios%20sectoriales/Notas%20de%20Investigacion/Ciberseguridad%20y%20ciberdefensa.pdf

❖ **Fase 0: Contextualización descriptiva funcional**

En esta fase, se plantea el contexto operacional y funcional del trabajo a realizar, identificando los ejes valorativos que señalaran los aspectos formales asociados con los marcos referenciales que se listan seguidamente: a) ¿Qué se quiere hacer?, b) ¿con que se puede hacer ?, c) ¿Cómo debe de orientarse o hacerse?, d) ¿Quién lo utilizara? y e) ¿cuál es su dominio, temporalidad e imagen con la que se proyecta su cadena de valor?

❖ **Fase 1: Estructuración funcional y convalidación teórica**

Producto de la construcción realizada en la fase anterior, se procede entonces a seleccionar, clasificar e interpretar la fundamentación teórica pertinente a los campos de la ciberdefensa y la ciberseguridad, catalogándose así procedimentalmente los mecanismos, servicios y estrategias que denotan el campo de aplicación de la Criminalística Computacional mediante la elaboración de un modelo objetivo que permita el tratamiento formal de las evidencias a la luz de la normativa legal considerada por los jueces de la república.

❖ **Fase 2: Construcción del referente sistémico**

La elaboración del modelo pretendido por este trabajo para el tratamiento logístico de las evidencias producidas por el acometimiento de un delito informático[5] valorado según la legislación existente, permite esquematizar funcionalmente los aspectos siguientes: a) Valoración teórica y experimental de los servicios y mecanismos de seguridad, b) tipología de ataque, c) estructura logística del vector de ataque, d) tecnología utilizada por el Hacker, e) valoración de resultados del ataque, f) estructuración y recopilación de evidencias y g) catalogación efectiva con visión jurídica de las evidencias acopiadas, razón por la cual el esquema producido se convierte en la base cibernética del prototipo del modelo que se construirá y validara, se reconocerá en esta base los aspectos relacionados con las variables identificadas, las funciones de proceso, la complejidad y estabilidad de los resultados producidos.

[5] Circunstancia de agravación punitiva, considerada como respuesta ponderable ante la acción cometida por un Ciberdelincuentes, cuyo proceder se sustenta por evidencias. http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

❖ **Fase 3: Diseño y construcción de la solución**

La consideración en el entorno de la Criminalística Computacional, mediante la construcción de un modelo validador que facilite la estructuración de evidencias para su posterior tratamiento ante un estrado judicial, según especificaciones de la informática forense, presupone el seguimiento y cumplimiento de estas actividades:

- Elaboración logística y procedimental de los ejes tecnológicos definidos para el acopio de evidencias, como resultado de las acciones forenses propias de un escenario computacional.
- Dimensionamiento operacional de las variables, procesos modificadores y salidas proyectadas, que involucran e integran fundamentos de la informática forense, la criminalística computacional, el pensamiento sistémico y la toma de decisiones para así elaborar, un modelo que represente la realidad estudiada con objetividad e integridad.
- Ponderación prospectiva de las funciones de relación y valoración generadas por la consideración de la integridad del vector de ataque formulado, la tecnología empleada y los resultados del desastre informático producido, identificando así las vulnerabilidades y el estado de la arquitectura o de la información estropeada producto de la acción producida por los piratas de la información.
- Formalización estructural del modelo, diferenciando los aspectos circunstanciales de carácter exógeno, los principios de valoración del impacto del desastre, la categorización del delito informático establecido y los procedimientos de recuperación y usabilidad del conjunto de evidencias que el perito en informática forense podrá utilizar como prueba final ante el Juez de la republica encargado de promulgar la sentencia correspondiente, al considerar el nivel punitivo de la acción.

❖ **Fase 4: Entrega de la solución: Criminalística Computacional: Modelo para estructuración de evidencias**

Habiéndose establecido el escenario para validación de la solución construida, y considerando como factores determinantes de su calidad y grado de usabilidad, se realizará ante la comunidad académica del programa y sociedad en general la presentación formal, para mostrar sus niveles diferenciadores sobre los que la evidencia, contemplada por el léxico de la criminalística computacional define su importancia y cadena de valor, como entidad de significancia para efectos legales que facilitan el juzgamiento del delito informático cometido.

1.6.3. RESULTADOS PROPUESTOS

El entregable del proyecto elaborado, permitirá al programa de Ingeniería de Sistemas de la Universidad Libre de Colombia obtener:

❖ Facilidad logística de intercambio con entidades gubernamentales y privadas que se ocupan de la ciberseguridad y la ciberdefensa, al compartir la integridad del modelo construido, cuya valoración jurídica certifique su probidad y confiabilidad.

❖ Catalogación de los servicios y mecanismos de seguridad, que permiten realizar con objetividad los procesos de acopio de evidencias dentro de la tecnología convencional y la tecnología del estado sólido, para evaluar jurídica y pericialmente los resultados de un desastre informático sobre los que opera la acción de un delito.

❖ Ponderación operacional de los esquemas y estrategias definidas para la ciberseguridad y la

ciberdefensa, que se establecen por sus características en el contexto nacional, para proyectar sistémicamente su adaptabilidad, usabilidad y amigabilidad convencional, al involucrar procesos destructivos que conllevan elementos punitivos con potencialidad de ser judicializados y sancionados legalmente por los Jueces de la República.

1.6.4. FASE TEÓRICA PARA EL ANÁLISIS PROCEDIMENTAL

El escenario de acción operacional y logística funcional investigativo, que permitirá construir el modelo para la estructuración de evidencias, según principios de la informática forense y la seguridad digital, involucran el tratamiento e instrumentación analítica de las disciplinas señaladas con ayuda de la figura 1, la teoría que determina los aspectos básicos de la modelación, presupone el manejo interpretativo de los núcleos descriptivos asociados con: a) vector de ataque, b) especificación de dominio, c) puertos bien conocidos (Well Known Ports), e) canales de conversación en tiempo real (News. http://xnews.newsguy.com, herramientas de valoración y exploración de rutas (Netscan Tools y exploración DNS. www.netscantools.com), g) interpretación de la huellas de salto de un paquete junto con las debilidades de respuesta generadoras de vulnerabilidad (página web, Shellcode).

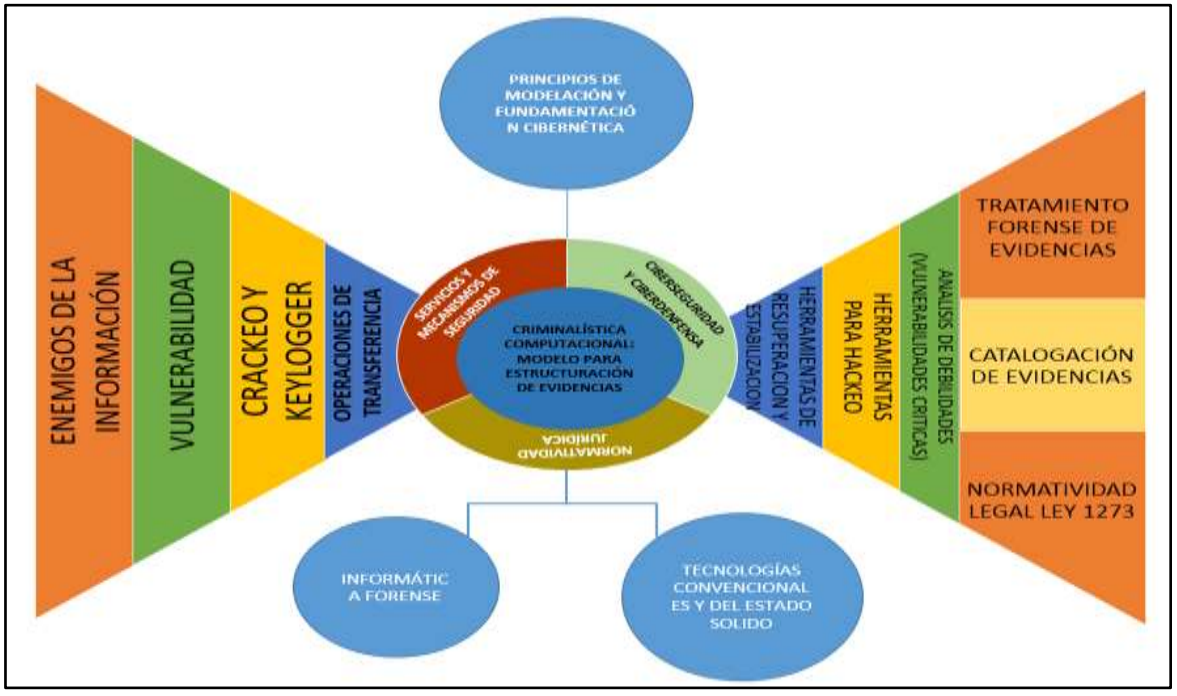


Figura 1: Fundamentación Teórica Disciplinar

Fuente: Aporte Realizadores

Complementariamente, se hace indispensable evaluar los correspondientes factores que definen el marco crítico de significancia teórica, que a la postre determinan la base analítica de sustentación experimental, a saber:

- ❖ Principios normativos RFC2828[6], X800[7] y X.509[8]
- ❖ Reguladores operacionales para servicios y mecanismos de seguridad.
- ❖ Estructuración logística de la evidencia procedimental en el entorno jurídico: mantenimiento cadena de custodia[9].
- ❖ Descriptores en conjunto de las operaciones generadas por los hackers en sus vectores de ataque cuyo efecto destructivo generan la tipificación punitiva.
- ❖ Perfiles potenciales del delincuente informático como usuario directo de la tecnología de ataque.

El correspondiente marco de integración interpretativa, se presenta en la figura 2

[6] Vademécum que define el conjunto procedimental de seguridad promulgado por las agencias rectoras en internet. https://www.ietf.org/rfc/rfc2828.txt

[7] Modelo descriptivo de la seguridad de sistemas abiertos que operan sobre internet. https://www.itu.int/rec/T-REC-X.800-199103-I/es

[8] Plataforma logística que controla y regula la generación de certificados requeridos para implementaciones regulares de comercialización sobre internet. http://www.ipsec-howto.org/spanish/x532.html

[9] Procedimiento o entidad descriptiva de la fenomenología investigada para sustentar la acción de un delito cuya validez jurídica se interpreta mediante leyes de la república.
http://www.fiscalia.gov.co/en/wp-content/uploads/2012/01/manualcadena2.pdf

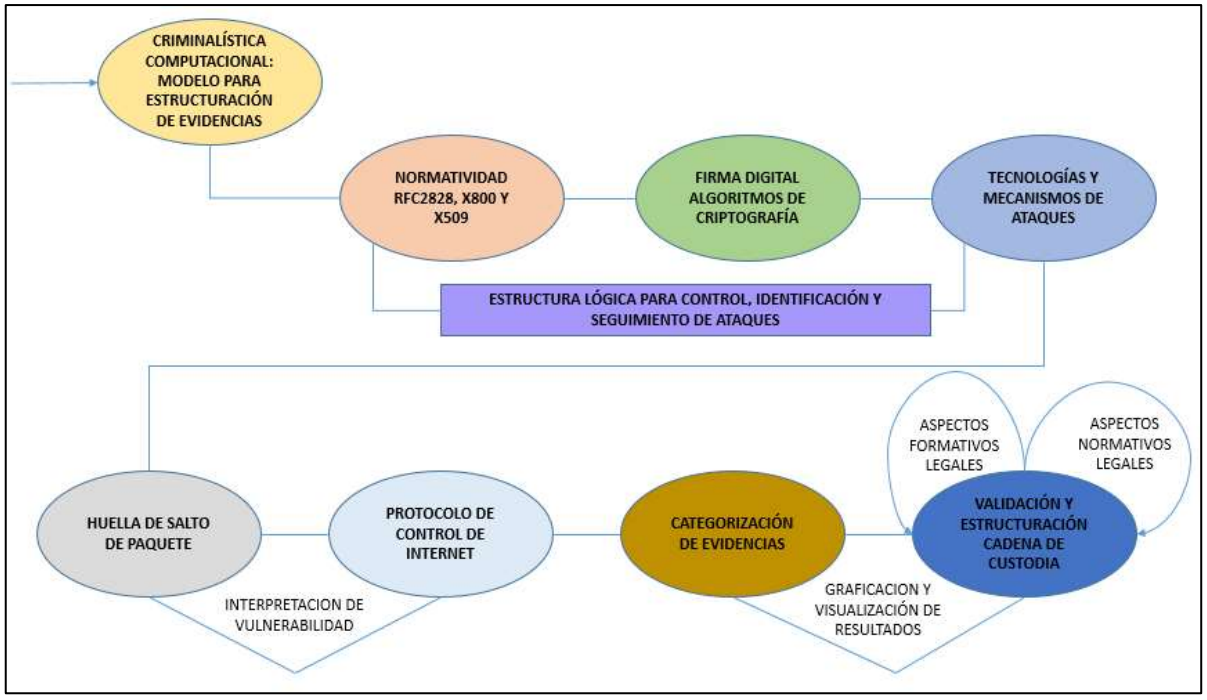


Figura 2: Integración Interpretativa Referencial

Fuente: Aporte Realizadores

2. ESCENARIO OPERACIONAL DE LA SEGURIDAD

El tratamiento e interpretación lógica y sistémica de la seguridad computacional, como plataforma proyectiva para la estructuración de la evidencia como entidad sustentadora del delito informático y como entidad de carácter analítico y decisional al interior de la informática forense, exige que evalué y dimensione la fundamentación teórica y conjunto de principios operacionales asociados con los mecanismos y servicios de seguridad, para elaborar el referente funcional que cataloga el accionar de los piratas de la información y por ende dilucidar la valides y pertinencia de las herramientas forenses con las cuales se puede elaborar y dilucidar una evidencia cuya integridad permite sustentar jurídicamente un delito, elementos procedimentales de análisis, que se exponen como la piedra angular que sustenta la logística de la seguridad informática.

2.1. ASPECTO PROCEDIMENTAL DE LA SEGURIDAD

Formalmente en el universo computacional, la seguridad se interpreta como la entidad estructural, cuyas políticas y mecanismos, traslucen lógicamente la confidencialidad e integridad [Tanenbaum 2012].

La política de seguridad describe: a) Acciones permitidas en el sistema, b) Acciones restringidas y c) Actividades de respuesta a contingencias

El mecanismo, es entonces el vehículo de implementación de la política y técnicamente referencia los facilitadores listados aquí: a) Cifrado, b) Autenticación, c) Autorización y d) Auditoria

La consideración sistémica de las políticas y mecanismos de seguridad, permiten validar con determinación las llamadas amenazas de seguridad, manifestadas operacionalmente en estos factores o caos de manifestación: a) Intercepción, b) Intercepción, c) Interrupción y d) Modificación, e) Modificación y f) Fabricación. [Pfleeger 2006].

Con ayuda de las figuras 3 y 4, se visualiza tanto la valoración del mecanismo, como la manifestación de la amenaza de seguridad, su interpretación permite extraer las características asociadas con los métodos de protección contra las amenazas, entre las que se encuentran [Doorn y Rivero 2002]:

- Protección contra operaciones invalidas

- ❖ Protección contra invocaciones no autorizadas
- ❖ Protección contra usuarios no autorizados

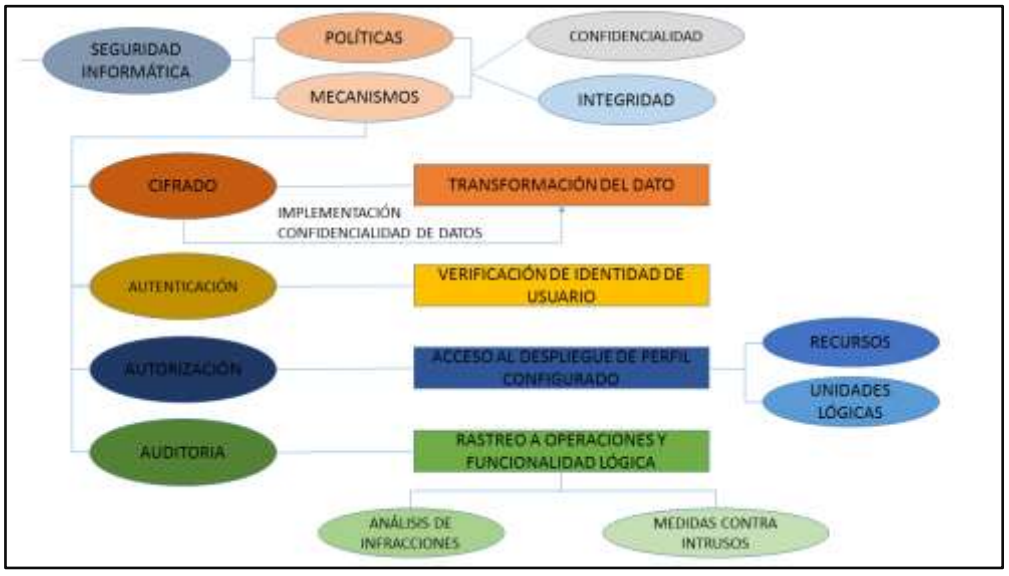


Figura 3: Valoración del Mecanismo de Seguridad

Fuente: Construcción Propia

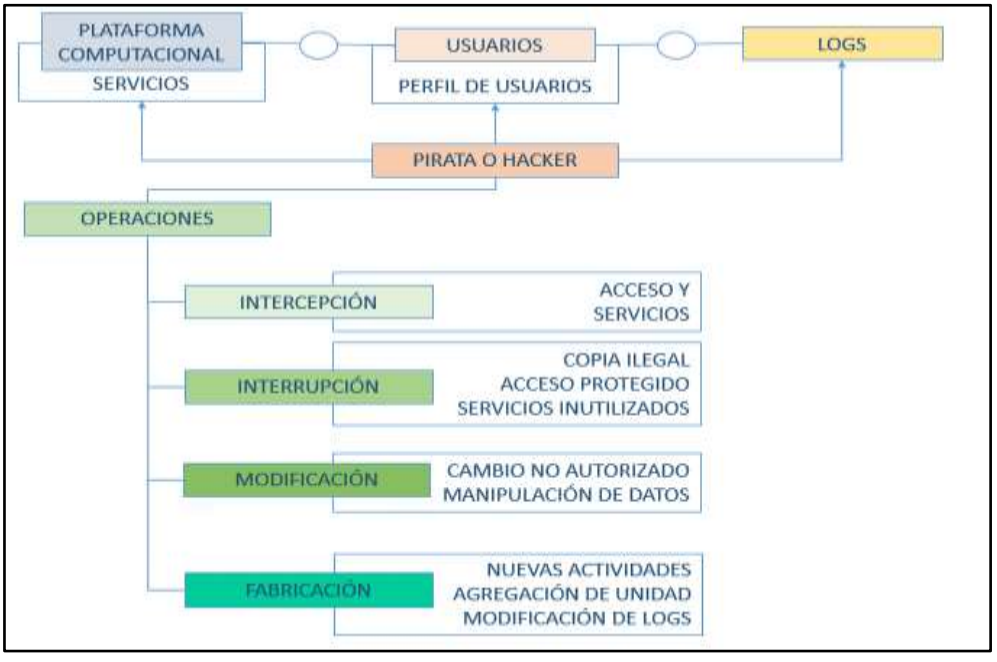


Figura 4: Manifestación de Amenazas

Fuente: Aporte Realizadores

2.1.1. PATRON LOGICO DE SEGURIDAD

El patrón lógico de seguridad, estructura tanto el esquema normativo de operación como la arquitectura de seguridad; la valorización de la arquitectura, conlleva la interpretación de la organización por capas y la distribución de mecanismos [Gollmann 2006], un esquema normativo de seguridad identifica los factor generador semánticos, es decir los núcleos de catalogación, núcleos fácilmente encontrados en la conocida arquitectura GLOBUS[10] y que se listan a continuación.

- Composición y direccionamiento de múltiples dominios lógicos.
- Existencias de políticas de seguridad local.
- Valoración operacional con iniciadores conocidos en todos los dominios.
- Toda operación requiere autenticaciones mutuas.
- La autenticación global reemplaza a la local.
- El control de acceso depende de la seguridad local.
- Un usuario cataloga y delega derechos a un proceso.
- Se comparten credenciales en grupos de procesos definidos en el mismo dominio.

Los componentes del patrón lógico, se visualizan en la figura 5, pudiéndose calificar así, integridad de la política de seguridad implementada.

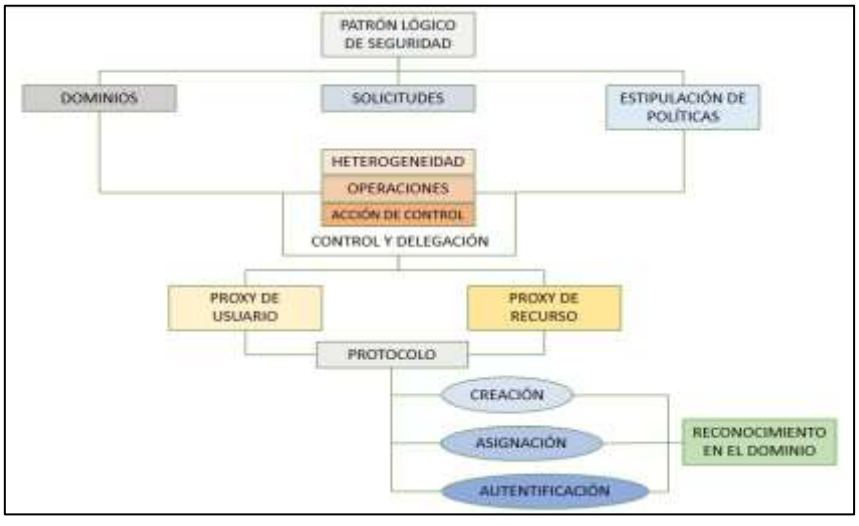


Figura 5: Componentes Patrón Lógico de Seguridad

Fuente: Aporte Realizadores

[10] Sistema de área amplia para catalogación de seguridad en sistemas distribuidos. The Data Grid. Chervenak A. and Foster I.

2.1.2. DISTRIBUCION DEL PATRON DE SEGURIDAD

El patrón de seguridad que se configura en una arquitectura computacional, identifica su lógica de operación en tres grandes núcleos: [Bishop 2006]

- NIVEL DE CONFIGURACION MECAMATICO (SOPORTE LOGISTICO OPERACIONAL)
  - Hardware
  - Kernel del Sistema Operativo
- NIVEL LOGISTICO FUNCIONAL
  - Servicios del Sistema Operativo
  - Middleware
- NIVEL DE APLICACIÓN

La figura 6, ilustra esta distribución; dicha distribución, esta soportada en dos grandes grupos de protocolos, los de bajo nivel y los de alto nivel, su espectro de operación se asocia así:

- Protocolo de bajo nivel
  - Nivel de configuración Mecamatico (Soporte Logistico Operacional)
  - Nivel logístico funcional
- Protocolo de alto nivel
  - Nivel logístico funcional
  - Nivel de aplicación

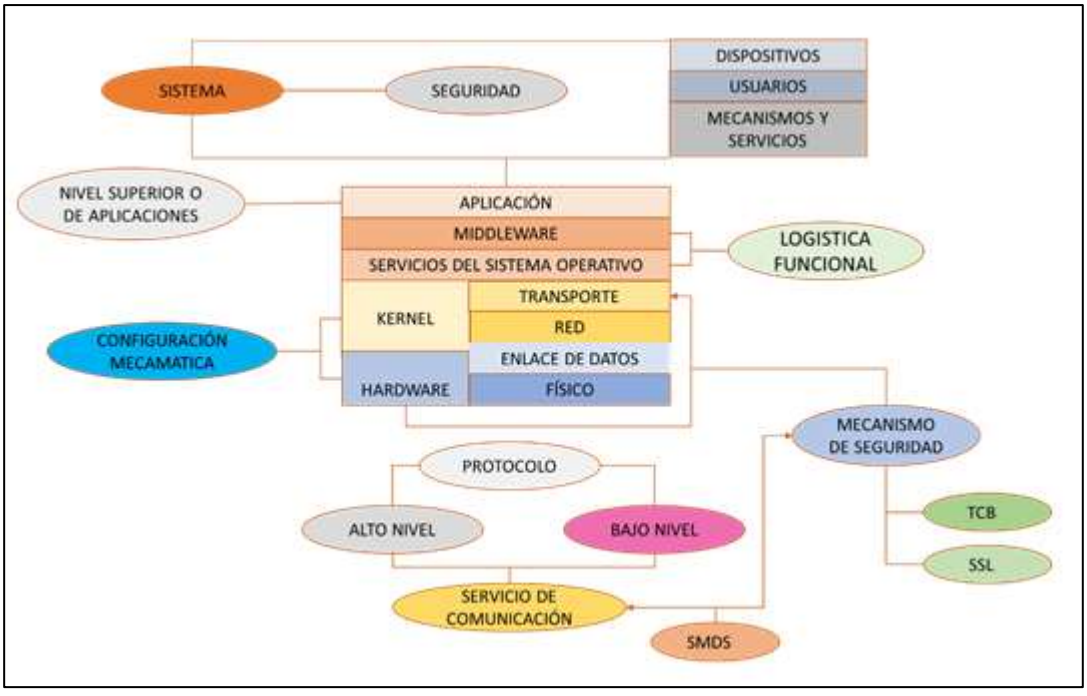


Figura 6: Distribución Patrón de Seguridad

Fuente: Aporte Realizadores. Modificación original Andrew Tanenbaum

2.1.3. FOCO OPERACIONAL DE ATAQUE

El rompimiento del escudo de seguridad por parte del hacker, genera entropía en la fiabilidad del sistema [Kopetz 2003], afectando plenamente los factores de disponibilidad, confidencialidad y mantenimiento.

La disponibilidad, presupone la disposición de utilización inmediata del equipo, la confiabilidad alude el funcionamiento continuo y el mantenimiento define la facilidad de reparación ante la ocurrencia de una falla o error, bien sea de carácter transitorio, intermitente o permanente [Tanenbaum 2012].

La taxonomía de las fallas, permite identificar cinco focos o núcleos a saber:

- De congelación
- Omisión
- Tiempo
- Respuesta

- Arbitrario

El marco descriptivo de cada tipo de falla se define en la figura 7.

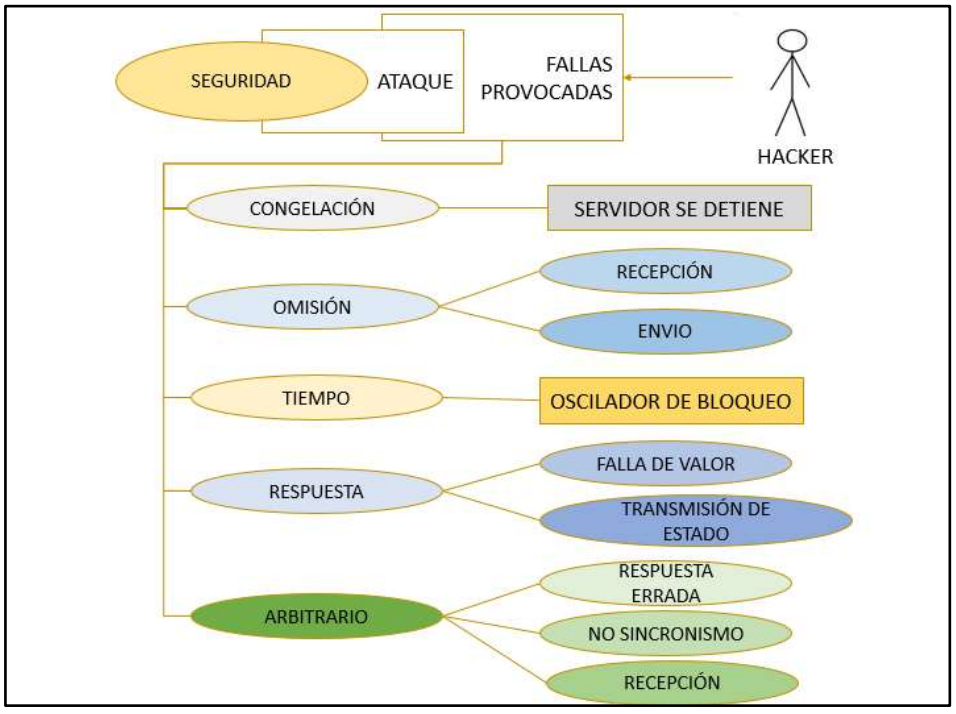


Figura 7: Semántica de Fallas Computacionales

Fuente: Aporte Realizadores

El foco operacional de ataque, se contrarresta al establecer canales seguros y al catalogar estos factores:

- Autenticación :a) Clave secreta compartida, b) Distribución de claves por protocolo NS (PANS) y c) Criptografía con clave publica
- Confidencialidad : a) Firma Digital y b) Clave de sesión
- Comunicación segura
- Control de acceso: a) Dominios de protección, b) Cortafuegos (Firewall) y c) Protección de agente
- Administración de claves
- Administración de autorización: a) Capacidad de propietario, b) Certificado de atributo y c) Delegación por Proxy.

2.2. MARCO DE ESPECIFICACION LEGAL

El gobierno nacional, con la ley 1273, tutelo la información como bien jurídico y contemplo en su articulado, la tipificación de los delitos configurados al producirse un ataque, por acción del hacker, significando entonces que el actuar del experto en informática forense, podrá acopiar las evidencias relacionadas con los ejes de acción que se listan:

- Acceso abusivo a un sistema de información
- Obstaculización ilegitima de un sistema informático
- Interceptación de datos informáticos
- Daño informático
- Uso de software malicioso
- Violación de datos personales
- Suplantación de sitios web
- Circunstancias de agrupación permitir
- Hurto por medios informáticos
- Transferencia no consentida de activos

En el anexo 1, se presenta el contenido de dicha ley, con ayuda de la figura 8, se muestra la tipificación de la acción legal frente a un ataque informático.

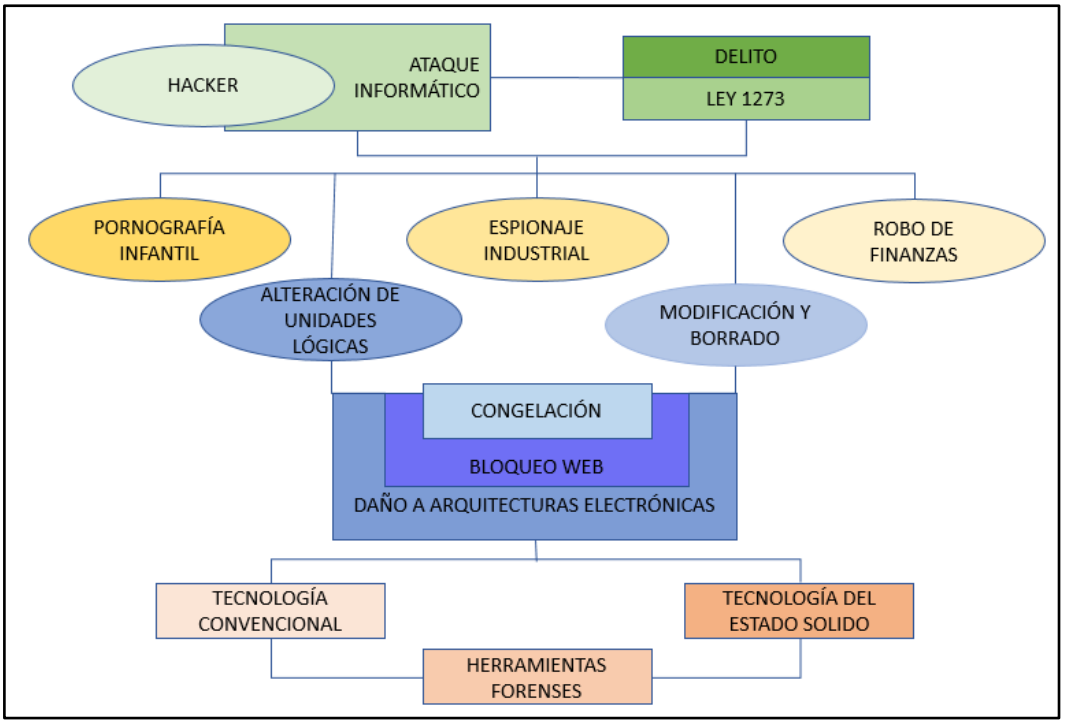


Figura 8: Configuración de Tipificación Legal

Fuente: Aporte Realizadores

En el campo del tratamiento de evidencias, para su correspondiente mapeo jurídico según artículo de dispuesto en la ley 1273, el experto en informática forense, deberá dominar con objetividad esta temática.

- Amenazas modernas de seguridad
- Aseguramientos de dispositivos en la red
- Autenticación, autorización y auditoria
- Implementación de tecnologías firewall
- Aseguramiento de LAN
- Sistemas criptográficos
- Implementación de VPN
- Administración de redes seguras
- Implementación de tecnologías IPS

La estructuración de evidencias, exige que el experto este familiarizado con: a) Plan de Desastre: que se hace cuando se pierde la información, b) Plan de Recuperación del Desastre: que se usa para

restablecer el sistema, c) SLA (Service Level Agreement): Calidad, tiempo, documentación, y disponibilidad funcional, y d) Set Operacional Biométrico.

El Set operacional biométrico, determina en el experto forense quien pretende estructurar las evidencias relacionadas con un caso de estudio, el conocer:

- HAND GEOMETRY: identificación al usuario por la forma de las manos
- IRIS IMAGING: Digitalización de la imagen del Iris
- RETINA TECOGNITION: Patrón único de Retina
- SIGNATURE VERIFICATION: Verificación de firma digital
- SPEAKER RECOGNITION: biometría de la voz

De igual manera, se hace imprescindible el reconocimiento y familiarización con la operación de estos Firewall, a saber:

- Control de servicios
- Control de usuarios
- Control de comportamiento

El marco referencial de acción legal, para poder estructurar el escenario de evidencias, presupone el conocimiento de los ejes de contextualización que se señalan:

- Ámbito de aplicación
- Responsable política de seguridad
- Nivel de operación de la acción
- Responsable de la seguridad
- Integridad de las políticas de seguridad
- Base tecnológicas de apoyo: a) SNORT, b) NESSUS, c) HONEYD, d) SAMHAIN y e) OSSEC

- ❖ CATALOGO DE SEGURIDAD: a) Fiabilidad, b) Facilidad de uso (amigabilidad), c) Mecanismo de prevención d)Aceptación y e) Estabilidad
- ❖ ISO / 17799[11]
  - o Políticas de seguridad
  - o Organización seguridad
  - o Gestión de Activos
  - o Cifrado
  - o Control de acceso
  - o Seguridad física
  - o Seguridad en comunicaciones
  - o Gestión de incidentes
  - o Aspectos de seguridad
  - o Conformidad
- ❖ Normatividad referencial: a) RFC 2828, b) X:800, c) X.509 y d) RFC 2574, e) RFC 3227
- ❖ Escenario de la aplicación de la seguridad: a) Correo electrónico , b)WEB, c) IP y d) Nube

2.2.1. FORMALIZACION DE LA EVIDENCIA

En el contexto jurídico, la evidencia se define como la certeza manifiesta que resulta innegable al no admitir la duda, catalogándose como prueba determinante en un proceso judicial; esta certeza manifiesta proviene de:

- ❖ Escena del ataque
- ❖ Victima referencial del ataque

[11]Norma que define los procesos de implementación de sistemas de gestión para la seguridad de la información http://www.iso.org/iso/catalogue_detail?csnumber=39612

- Presunto responsable o autor

El indicio o evidencia, estructurada por el investigador forense, por sus características puedes ser determinable, si se construye luego de un análisis minucioso o a simple vista e indeterminable, si se demanda la aplicación del análisis complejo, validándose también su directa asociatividad o su no asociatividad, por ejemplo, si el hacker borra archivos, los indicios asociados se definen entorno al dispositivo, al MRB(Master Record Boot) y al integrador de almacenamiento (FAT32, VFAT, EXT2), pero los no asociativos, serán; fuente de alimentación, parámetro MTBF[12] del disco, velocidad y latencia.

Con ayuda de la figura 9, se presenta el movimiento requerido para elaborar la evidencia, que se habrá de utilizar para sustentar jurídicamente la acción del delito cometido; el trabajo en el escenario de la informática es aplicado en el campo jurídico convencional, pues es necesario seguir o realizar estos procedimientos:

a- Observar la escena del ataque, para determinar y definir que objetos serán parte de la evidencia.

b- Buscar y descubrir evidencias de acción analítica.

c- Recolectar dichas evidencias, marcando tanto el espacio referencial como la evidencia.

d- Visualizar el escenario con fotos o videos.

e- Seleccionar las herramientas que se emplearan para la recolección de evidencias.

f- Especificación de la unidad contenedora de la evidencia, para garantizar la integridad mediante sello y firma de constatación, recolectando solo los elementos relacionados con el hecho que se investiga.

[12] MTBF: Acrónimo ingles que señala el tiempo promedio de fallas del disco. http://edinn.com/es/mtbf-mttr.html

Figura 9: Procedimiento Elaboración Evidencia

Fuente: Aporte Realizadores

g- Analizar el resultado de la Inspección, implementando técnicas de planimetría si lo requiere el caso.

h- Elaboración del informe Técnico.

i- Cotejación estructural de la validez y pertinencia de la evidencia, para verificar la conducta punible [Iguaran 2012].

j- Verificación del estado de la evidencia digital [Lopez 2003]

- ❖ Almacena miento estático o con atributo persistente.
- ❖ Almacena miento dinámico temporal o volátil.
- ❖ Tránsito o desplazamiento.

k- Valoración de la cadena de custodia (CDC): a) Extracción, b) Preservación, c) Traslado, d) Entrega a autoridades y d) Custodia

El contenido teórico expuesto, puede ser ejemplificado con el análisis del siguiente caso:

1- Se ejecuta una tarea programada que lleva el disco con múltiples archivos.
2- Se modifica el horario del sistema.
3- Se reinicia continuamente el sistema.

La recolección de la evidencia, se fundamentara en el seguimiento de estas faces, a saber:

- Identificación del desastre o problema
- Selección acción de contingencia
- Indagación procedimiento de catalogación del ataque
- Fijación mecanismo correctivo
- Muestreo referencia

l de implicados
- Determinación escudo procedimental de recolección de evidencias
- Elaboración de informe técnico
- Manifiesta cadena de custodia

Acciones que se valoran sistemáticamente de esta manera:

a- En el Kernel CD/Windows/system32

Ejecutar compmgmt.exe y seleccionar el programador de tareas para evaluar el resumen tal como lo muestra la figura 10

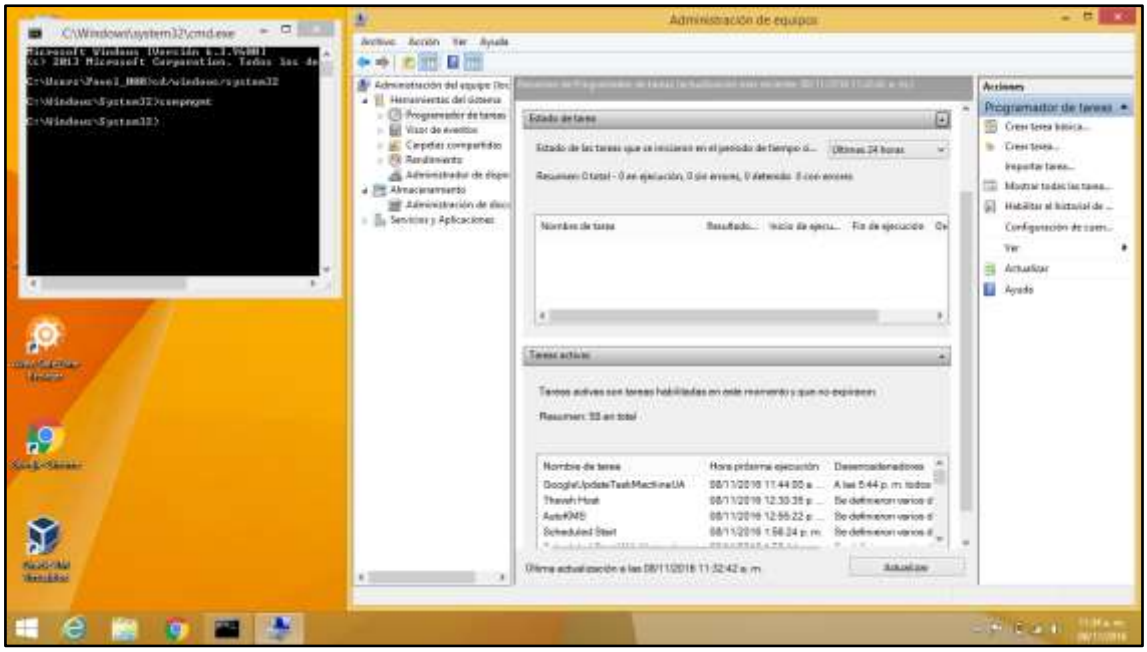


Figura 10: Resumen del Programador

Fuente: Aporte realizadores

b- Mapear el seguimiento de creación para observar el desencadenador de tarea (ver figura 11)

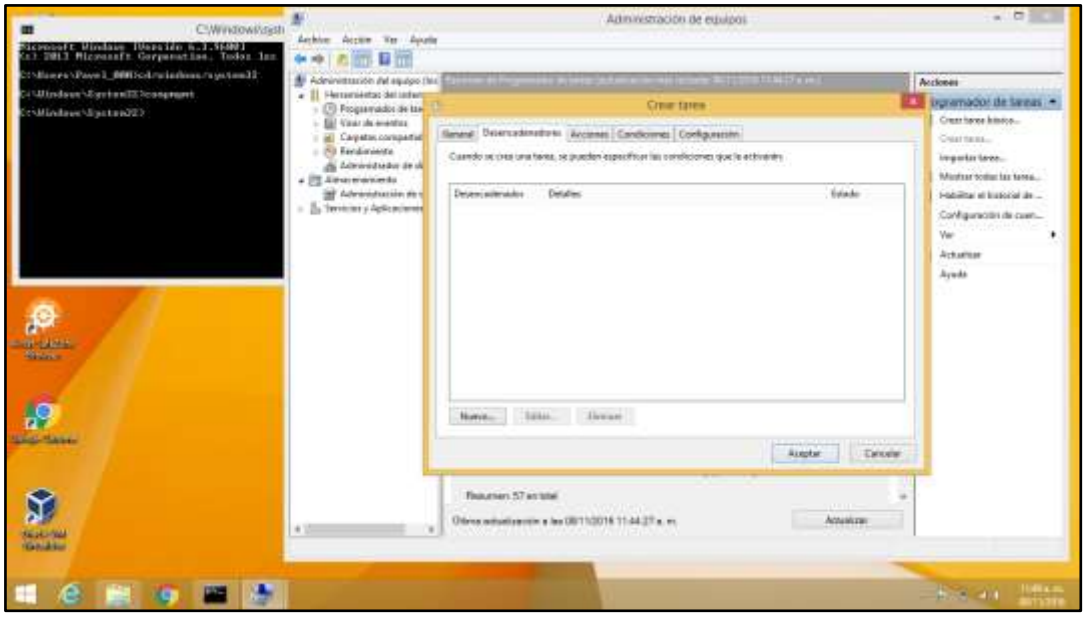


Figura 11: Desencadenador de Tareas

Fuente: Aporte Realizadores

c- Evaluar directorios configurados y observar contenidos de Script, por ejemplo, si se encuentra este:

```
Set wshshell = wscript.CreateObject("WScript.Shell")
wshshell.run "https://youtu.be/cNm6XTdycoo"
Wshshell.run "notepad"
wscript.sleep 400
wshshell.sendkeys "Esta"
wscript.sleep 300
wshshell.sendkeys "~computadora"
wscript.sleep 300
wshshell.sendkeys "~se daño y no sirve"
wscript.sleep 300
wshshell.sendkeys "~Pavel y Jennifer, ustedes me atacaron"
wscript.sleep 300
wshshell.sendkeys "~no se que hacer"
wscript.sleep 300
wshshell.sendkeys "~quede sin control"
wscript.sleep 300
wshshell.sendkeys "~ayuda, ayuda"
wscript.sleep 300
wshshell.sendkeys " "
wscript.sleep 300
wshshell.sendkeys " "
wscript.sleep 300
wshshell.sendkeys "~que me esta  pasando?"
wscript.sleep 600
wshshell.sendkeys "~Pavel y Jennifer no me dejen"
wscript.sleep 100
wshshell.sendkeys "O"
```

```
wscript.sleep 100
wshshell.sendkeys "O"
dim uno, dos,k
k=1
uno=" Pavel y Jennifer son los culpables de este ataque"
set dos=createobject("sapi.spvoice")
while k<10
dos.speak uno
k=k+1
wend
do
wscript.sleep 50
wshshell.sendkeys "O"
loop
```

Se encuentra y se pondera la evidencia en el ataque pero si se valida la existencia de este soporte

```
#include <conio.h>
#include <stdio.h>
#include <stdlib.h>
#include <windows.h>
#include <io.h>
#include <dir.h>
#include <sys\stat.h>
#include <string.h>

main()
{

    int k,l;
    char texto[10]="libre", sale[10], otro[10]="libre";
```

```
char salida[80]="sueña como si fueses a vivir toda la vida";
FILE *uno;
for (k=0;k<100;k++)
{

itoa(k,sale,10);
strcat(texto,sale);
printf("%s\n",texto);
if((uno=fopen(texto,"w"))==NULL)
{
printf("error al abrir archivo");
getch();
exit(1);
}
for(l=1;l<2000;l++)
fputs(salida,uno);
strcpy(texto,otro);
 }
getch();
   system("del li?*.*");
return(0);
}
```

Entonces, se deberá emplear un instrumento o herramienta para su validación operacional.

d- Confirmación resultado y documentación de acción, tal como se muestra en la figura 12 y 13

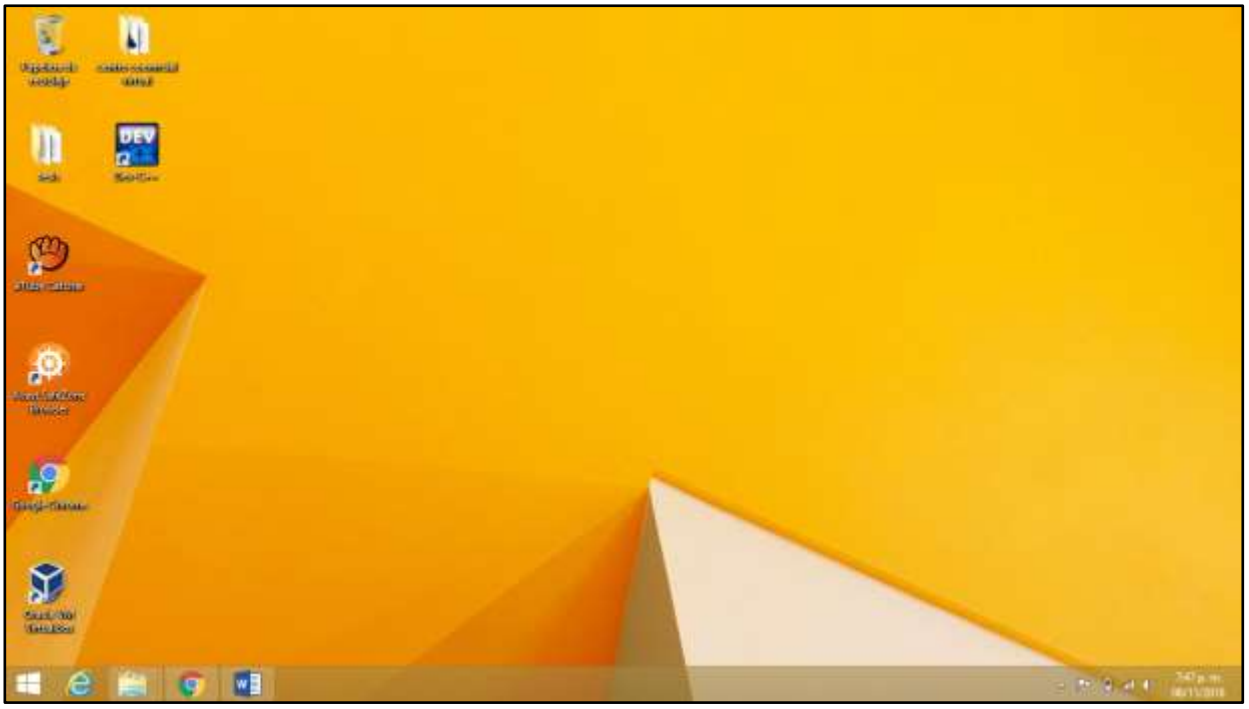


Figura 12: Estado Antes del Ataque

Fuente: Aporte Realizadores

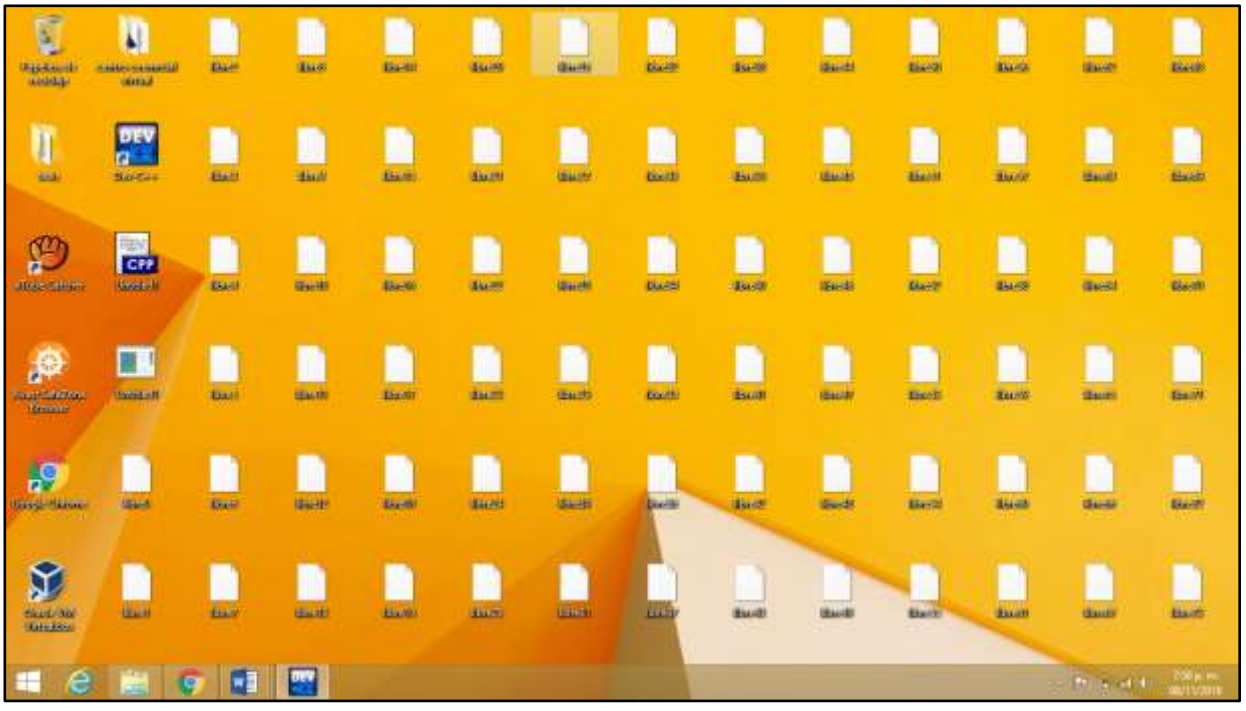


Figura 13: Estado Después del Ataque

Fuente: Aporte Realizadores

e- Describa evidencia a partir del indicio recogido.

f- Tipifique el delito cometido y elabore documento.

2.2.2. HERRAMIENTAS PARA SOPORTE FORENSE

La construcción de evidencia, hace que el investigador forense, se encuentre familiarizado con la operación de:

- Estación Forense Velociraptor 7
  - Almacenamiento de evidencias de 32TB en Raid 5.
  - SSD de 2TB en Raid 0 para el S.O. RAM de 256GB.
  - DeepSpar para recuperación de archivos en discos dañados.
  - Puertos bloqueados contra escritura FireWire, USB 3.0, SATA, eSATA.
  - Refrigeración líquida, menos ruido y máximo rendimiento.
- Duplicadora Logicube modelo Forensic Talon Ultimate
  - Velocidades cercanas a los 23GB/min.
  - Su modelo estándar incluye soporte SATA, IDE y USB3.0. Se pueden añadir módulos para soporte SAS y FireWire.
  - Permite hacer imágenes a partir de una fuente con hasta 3 destinos.
  - Cifrado AES 256.
  - Interfaz basada en web, fácil de usar. Permite acceso remoto mediante un navegador web.
- PC-3000 Express System
  - Funcionalidad Basada en enlace a puesrtos SATA e IDE
  - Almacenamiento amplio de hasta 6 TB
  - Recuperador incorporado medinate la solución Data Extractor Express
- Duplicadora Voom modelo Hardcopy 3
  - Velocidad de hasta 7.5 Gb por minuto en la transferencia de datos.

- Realiza 2 copias a la vez de un mismo disco duro.
- Verificación SHA256.
- Modos de duplicación (clonación y creación de imágenes).
- Copia DCO y HPA (copia todos los datos incluidos los protegidos).
- Diferentes métodos de borrado.
- Duplicación de otros discos duros (ATA, portátiles...).
- Ingeniería de duplicación de discos.

Pero se requiere tener conocimiento también de estos soportes:

- ❖ Adquisición y análisis de memoria.
  - PD
  - FTK imager
  - RedLine
  - Memorize
- ❖ Montaje de Discos
  - OSFMount
  - FTK imager
  - VHDTool
  - LiveView
- ❖ Carving
  - PhotoRec
  - RecoverRS
  - NTFS Recovery
  - IEF
- ❖ Soporte de archivos
  - analyzeMFT
  - MFT_Parser
  - Winprefectchview
- ❖ Analisis de Malware

- PDF Tools
- Firebug
- IDA Pro
- OfficeMalScanner
- shellcode2exe

❖ Frameworks
- PTK
- DFF
- OSForensics

❖ Analisis registro de Windows
- RegRipper
- WRR

❖ Herramientas de Red
- Xplico
- Splunk
- AlientVault

❖ Recuperacion de contraseñas
- Ntpwedit
- Ntpasswd
- pwdump7
- OphCrack
- L0phtcrack

❖ Acceso a dispositivos móviles
- Iphone
  - iPBA2
  - iPhoneBrowser
- BlackBerry
  - MagicBerry
  - Phoneminer
- Android
  - Androguard

- Viaforensics
- Osaf

2.3. ESCENARIOS GENERADORES DE EVIDENCIAS

Para los propósitos de este trabajo, un escenario generador es el espacio u objeto que puede ser impactado o la acción de un vector de ataque configurado por el hacker, con el fin de modificar, destruir o congelar un valor informático o arquitectura telemática.

Según se afirma con la descripción anterior estos escenarios pueden ser [Tanenbaum 2012]

- Pc o Workstation
- Disco o raid de discos
- Multitransmisión atómica
- Semántica RPC (remote procedure call)
- Realización bifásica (2pc:two phase commit protocol)
- Generación de claves
- Matriz de control de acceso (ACL Access control list)
- Sistema de archivos distribuidos basado en Cluster
- Semántica de archivos corporativos
- Sistemas basados en la web
- Cache de proxy web
- Enrutamiento basado en contenidos
- Distribución y replica tuplas
- Correo electrónico
- Entorno IP
- Entorno de la nube

El listado anterior, responde a generadores convencionales, pero los que se listan a continuación, poseen un espectro de mayor complejidad en su tratamiento, pues se enmarcan en el plano de la protección bidireccional, dado que involucrado el papel de flujo óptico, tal como se muestra aquí; [Capmany y Ortega 2010]:

- ❖ Path Protection (conmutación de camino)
- ❖ Span Switching (conmutación de enlace)
- ❖ Ring Switching (conmutación de anillo)
- ❖ Esquemas de protección OMS:1+1, OMS:1:1, OMS-DPRING, OMS-SPRING

Pero también se hace necesario entender los problemas que se presentan al atacar una red de acceso, entendido como el conjunto de elementos que permiten conectar a cada abonado con el centra local de la cual depende [Capmany y Ortega 2010], dado que el vector de ataque puede definir como objetivo de destrucción o congelación:

- ❖ Procesos de trasmitir, conmutación enrutamiento y multiplexación.
- ❖ Calidad del servicio.
- ❖ Protocolos de acceso.
- ❖ Autenticación en redes.
- ❖ Autenticación en redes: ADSL, XDLS, VDLS, FTTX (ver figura 14)

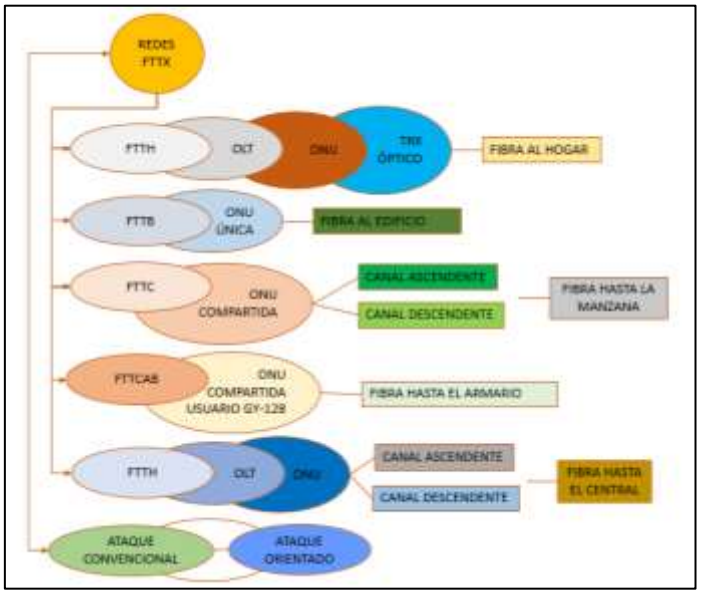


Figura 14: Tipologías FTTX Redes de Acceso

Fuente: Aporte realizadores

Jurídicamente entonces el experto en informática forense podrá enfrentarse con estas situaciones, situaciones que se convierten en focos generadores de evidencias, por ejemplo:

a- Alteración de la zona horaria para ejecutar programa perturbador
b- Borrado de archivos o mezcla de contenidos
c- Modificación de contenidos de archivo
d- Congelación cíclica de equipos.
e- Inyección SQL.
f- Modificación de conmutación de envió o enlace.
g- Congelación de un RAID.
h- fabricación de contenidos.
i- Alteración de transacciones o de la significación de un valor informático.
j- Bloqueo red de acceso.

k- Modificación pistas de reserva, de arranque o de servicio, congelación del bootstrap.

l- Alteración del selector del sistema de archivos (ver figura 15).

m- Ataques directos sobre tecnología de estado sólido.

n- Elevación de voltaje y destrucción del hardware mediante las llamadas Killer-USB.

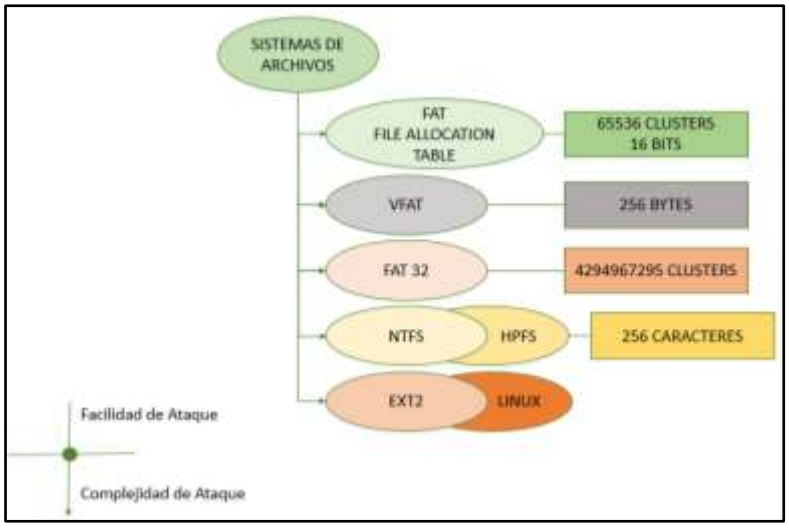


Figura 15: Referentes Típicos Sistema de Archivos

Fuente: Aporte realizadores

Quiere lo anterior decir que el delito informático, no solo se interpreta el validar el configurador dispuesto por la ley 1273, a saber: acceso abusivo, pornografía, robo de valores financieros o espionaje electrónico, pues cada configurante tipificado como delito, encierra factores singulares de validación.

2.3.1. EJEMPLIFICANTES LÓGICOS DE GENERACIÓN

Con los ejemplos siguientes, se muestra de manera elemental el proceso realizado por el experto forense, para evaluar el espacio geométrico del ataque y recuperar o estructurar la evidencia en su orden es:

- Caso 1: acción de lectura de un archivo por el intruso o fisgón
  - Actividad 1: se crea en Word el archivo pavel20.docx con 15 líneas.
  - Actividad 2: se guarda y unos minutos luego se le añade otro registro o línea.
  - Actividad 3: se utiliza una herramienta como METASHIELD ANALYZER y se observan los metadatos respectivos que se despliega en la figura 16.

Figura 16: Metadatos Encontrados Herramienta METASHIELD ANALYZER
Fuente: Aporte Realizadores

La evidencia sobre la trazabilidad del objeto modificado, se elabora a partir del metadato listado.

- Caso 2: apertura infinita de la unidad de CD/DVD con el Script jejis.vbs, que se lista aquí, se logra que la unidad de CD/DVD se abra y se cierre infinitamente, debiéndose apagar el equipo, pero como el ataque se implementa con hibernación se deberá optar por una acción especial.
  - Actividad 1: revisar el historial del programador de tareas.

- Actividad 2: encontrar el modulo invasor y retirar su residencia previa elaboración del informe respectivo, para consultar el log y señalar el fisgón o intruso.

```
'[1] MODULO DE VENTANAS
msgbox "Seguridad Informatica", 48,"Universidad Libre"
msgbox "Evidencias",20,"Delito Informatico!"

'[2] SEGMENTO DE ACTIVACION DE CD
Set OWMP = CreateObject("WMPlayer.OCX.7" )
Set colCDROMs = oWMP.cdromCollection
do
if colCDROMs.Count then
For i = 0 to colCDROMs.Count - 1
colCDROMs.Item(i).Eject
Next ' cdrom
End If
loop
'[3] MODULO DE ACTIVACION LEDS DE CONTROL
Set wshShell =wscript.CreateObject("WScript.Shell")
wscript.sleep 50
wshshell.sendkeys"{CAPSLOCK}"
wshshell.sendkeys"{NUMLOCK}"
wshshell.sendkeys"{SCROLLLOCK}"
```

Igual caso para recuperar la evidencia se ejemplifica con el código C++, que mantiene activa la pantalla, debiéndose probar todas las teclas.

```
#include <windows.h>
#include <conio.h>
#include <stdlib.h>
#include <stdio.h>
```

```
#include <time.h>
 void unilibre(int a, int b)
 {
 HANDLE libre;
 libre=GetStdHandle(STD_OUTPUT_HANDLE);
 COORD etm;
 etm.X=a;
 etm.Y=b;
 SetConsoleCursorPosition(libre,etm);
 }
 main()
{
   FreeConsole();
   srand(GetTickCount());
   int v1 = GetSystemMetrics(SM_CXSCREEN) - 1;
   int v2 = GetSystemMetrics(SM_CYSCREEN) - 1;
   system("color e2");
   while(!GetAsyncKeyState(VK_RSHIFT))
                                                                                {
      unilibre((rand() % v1) + 5, (rand() % v2) + 5);
      printf("Universidad Libre 2016\n");
      Sleep(5);
      system("cls");
      system("color a3");
      printf("Pavel y Jennifer Ing. Sistemas 2016\n");
      Sleep(3);
      printf("Gracias por utilizar nuestros servicios\n");
      Sleep(500);
      system("color d5");
      system("cls");
      system("color a3");
```

```
        printf("Ejemplo de3 programa perturbador, generador de evidencia\n");
        Sleep(3);
    return(0);
    }
```

- Caso 3: Modificación por agente externo del contenido de un archivo, cuyo registro almacena una descripción similar a:
    - Registro-Usuario
        - ✓ 3 Código usuario pic 9(5).
        - ✓ 3 nombusuario pic x (25).
        - ✓ 3 saldousuario pic 9(7) v 99.
        - ✓ 3 celuusuario pic x(10).

Si el intruso activa sobre el campo del saldo, borrando o aumentándolo. El experto deberá cumplir con estas tareas.

- Actividad 1: Listar copia del archivo según Backup reciente.
- Actividad 2: Listar última versión del archivo y comparar con el Backup.
- Actividad 3: Examinar código fuente del aplicativo.
- Actividad 4: Validar Log del sistema para cotejar interacción del usuario.
- Actividad 5: Explorar con Grupo de Desarrollo posibilidad de acción fraudulenta.
- Actividad 6: Elaborar informe sustentando y si se requiere inspección con apoyo psicológico se deben efectuar.

En resumen, la extracción de la evidencia, asociada con el ataque, considerara los elementos mostrados en la figura 17.

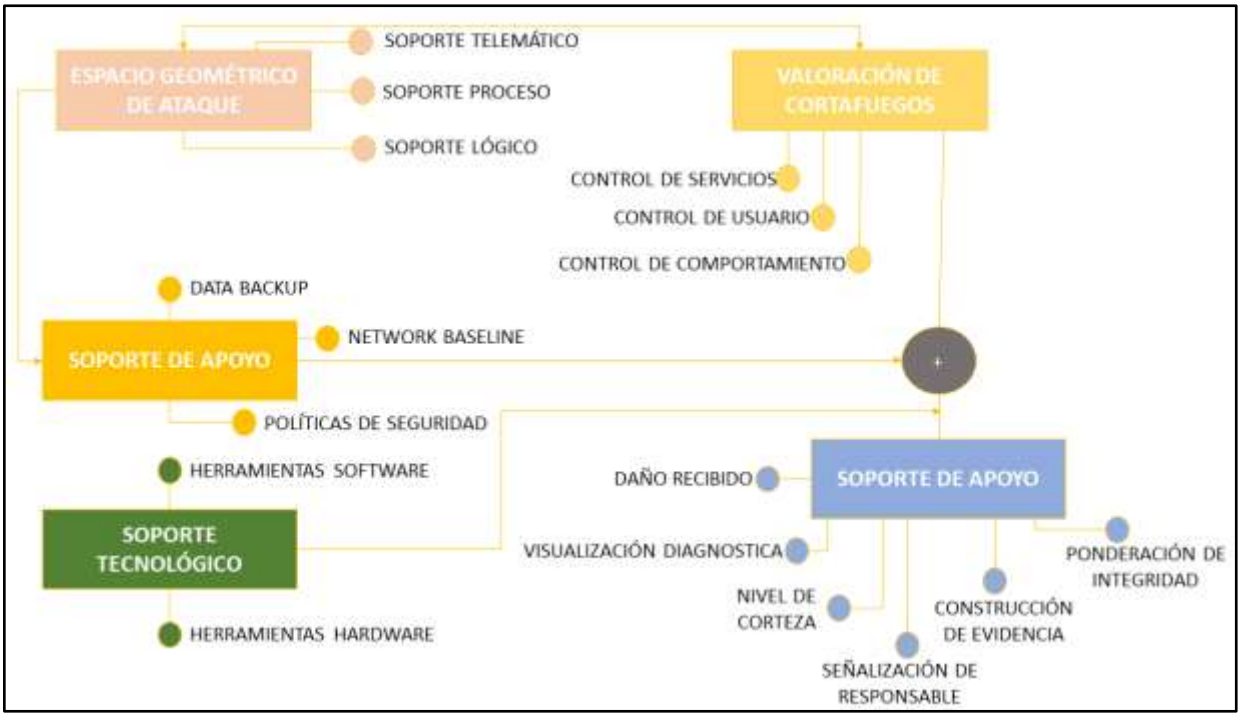


Figura 17: Patron Procedimental Extraccion De Evidencias

Fuente: Aporte Realizadores

2.3.2. INSTANTÁNEA OPERACIONAL DE SOPORTE

La construcción del soporte de indicio o evidencia, parte de la interpretación operacional del correspondiente eje de visualización y consulta, que permite al experto proyectar el esquema de análisis formal sobre el que se estructura la evidencia respectiva, esta instantánea o imagen de reseña lógica, permite cotejar tanto el andamiaje tecnológico como el articulado jurídico que debe ser referenciado, para ello. Entonces, interesado por construir la evidencia, posea el dominio completo de estos elementos del saber tecnológico.

- Modelo de grabación de Disco
  - FM: Frecuencia Modulada [Martin 2012]

    1 = PP (Dos Pulsos)

    0 = PN (Un pulso y una ausencia)
  - MFM: Frecuencia Modulada Modificada

    1 = NP (Ausencia y Pulso)

0 = si BIT anterior es 0, se codifica PN (pulso y ausencia), pero si el BIT anterior es 1 se codifica NN (ausencia de dos pulsos)

Por ejemplo será fácil para el experto forense, interpretar este contenido FM

PPPNPNPPPNPPPNPPPNPNPNPPPNPPPPPNPNPPPPPPPNPPPNPNPPPPPPPNPPPNPN

PPPNPNPPPPPNPNPNPPPPPNPPPNPNPNPPPNPPPPPNPPPNPNPPPN

Que almacena en hexadecimal el valor de: 4A454E4E49464552, cuyo equivalente es **Jennifer**; operación que se hará, en caso de haberse formateado el disco y querer recuperar su contenido.

- Principales puertos
  - 1/TCP = Multiplexor TCP
  - 7/TCP = Protocolo Echo (Eco) Responde con eco a llamadas remotas
  - 68/UDP= BOOTP BootStrap Protocol (Client), también usado por DHCP
  - 80/TCP = HTTP HyperText Transfer Protocol
  - 88/TCP = Kerberos Agente de autenticación
  - 110/TCP = POP3 Post Office Protocol (E-mail)
  - 123/UDP= NTP Protocolo de sincronización de tiempo
  - 177/TCP = XDMCP Protocolo de gestión de displays en X11
  - 443/TCP = HTTPS/SSL usado para la transferencia segura de páginas web
  - 500/UDP= IPSec ISAKMP, Autoridad de Seguridad Local
  - 514/UDP= syslog usado para logs del sistema
  - 587/TCP = SMTP Sobre SSL.
  - 690/TCP = VATP (Velneo Application Transfer Protocol)
  - 1080/TCP = SOCKS Proxy
  - 1433/TCP = Microsoft-SQL-Server
  - 1512/TCP = WINS Windows Internet Naming Service
  - 1701/UDP= Enrutamiento y Acceso Remoto para VPN con L2TP.
  - 1935/TCP = FMS Flash Media Server
  - 3128/TCP = HTTP usado por web caches y por defecto en Squid cache
  - 3306/TCP = MySQL sistema de gestión de bases de datos
  - 3389/TCP = RDP (Remote Desktop Protocol) Terminal Server

- 5060/UDP= Session Initiation Protocol (SIP)
- 5631/TCP = PC-Anywhere protocolo de escritorio remoto
- 8118/TCP = Privoxy

❖ Plano de control en redes IP [Capmany y Ortega 2012]

- Lectura de tablas de encaminamiento de los routers.
- Descubrimiento de conexiones directas con otros routers
- Encaminamiento , mediante identificación de estos protocolos: a) IGP (Interior Gateway Protocol), b) RIP (Routing Information Protocol), c) OSPF (Open Shortest Path First)

❖ Interpretación de norma UIT-T M.3400[13], para conocer las funciones de gestión en la red [Capmany y Ortega 2012]

- Gestión frente a fallas
- Gestión de configuración
- Gestión de contabilización
- Gestión de Prestaciones
- Gestión de Seguridad

❖ Identificación de mecanismos de protección

- SNCP(Subnetwork Connection Protection)
- MS-Spring/4 (Multiplexing Section Share Protection Ring)
- MS-Spring/2 (Multiplexing Section Share Protection Ring: 2)

❖ Compartimiento de firma secreta en servidores replicados

[13] Norma regulatoria del proceso de gestión y control en redes de computación. https://www.itu.int/rec/T-REC-M.3400/es

- Intercambio de claves Diffie-Hellman y distribución de claves secretas
    - Procedimientos para asignación de nombres, clase de manejadores de archivos, características de automontadores, semántica de archivos compartidos y bloqueo de archivos [Tanenbaum 2012]
- Referentes de contexto funcional [Froute 2013]
    - Policy tool
    - Protocolo SSL (Secure Sockets Layer)
    - Protocolo TLS (Transport Layer Security)
    - Generación de archivos de Certificados
- Interpretación lógico digital de las USB destructoras

  El experto forense, deberá estar familiarizado con el esquema lógico del circuito que soporta la operación de la conocida USB destructora cuya figura se muestra en la figura 18.

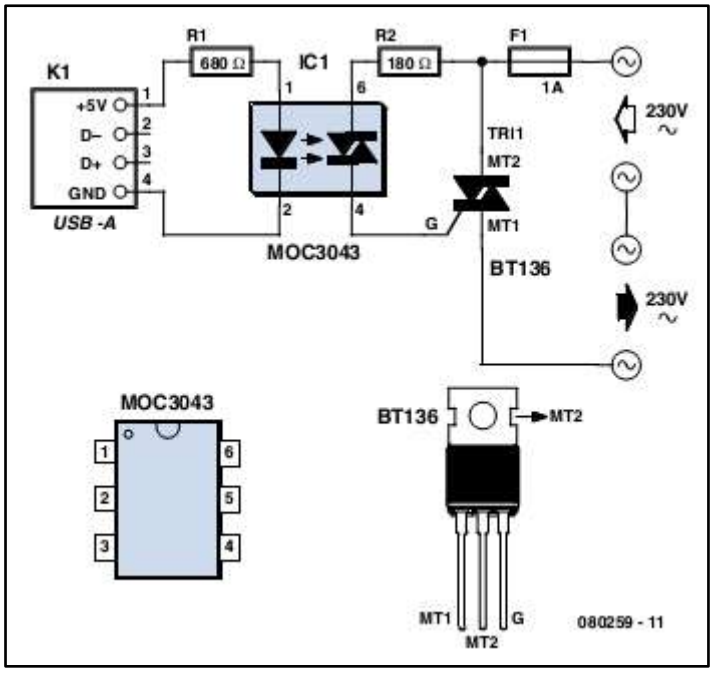


Figura 18: Estructura USB Destructora

Fuente: https://www.google.com.co/search?q=circuito+usb+killer

2.4. TRATAMIENTO JURÍDICO DE LA EVIDENCIA EN INFORMÁTICA FORENSE

Dentro del léxico pertinente al peritaje forense, el experto encargado de elaborar el indicio o evidencia, deberá tener presente estas características [Acurio 2013]:

- Objetividad: Observación código de ética
- Autenticidad: Validación de integridad
- Legalidad: Conocimiento de las leyes, para cumplir su articulado
- Idoneidad: Autenticidad, relevancia y suficiencia del medio estudiado

- ❖ Inalterabilidad: Cadena de custodia
- ❖ Documentación: Todo debe sustentarse mediante escritos entendibles con objetividad

El perito en informática forense, debe conocer que para su trabajo, el hardware se comporta como o mecanismo o producto del delito, pero que por sus propiedades es a su vez un instrumento y una evidencia es decir, reviste las mismas propiedades de la información [Agualimpia 2013], pero a su vez debe validar que la evidencia está directamente ligada al sistema computacional convencional o abierto, al sistema de comunicación teleinformática y al sistema convergente o de soporte móvil.

Básicamente, el actuar del experto forense puede hacerse con permiso directo del afectado o por toma precautelativa, en este caso se deberá operar con ayuda directa de la policía o agente de seguridad, elaborando el esquema respectivo que permitirá responder los siguientes interrogantes:

- ❖ ¿Cuándo y a qué hora se realizó el allanamiento?
- ❖ ¿Cómo se ingresó sin previo aviso?
- ❖ ¿Está preparado el soporte de cadena de custodia?
- ❖ ¿existen múltiples espacios de allanamiento?
- ❖ ¿Cómo se examinaran los equipos?
- ❖ ¿Cuáles requieren una orden especial?
- ❖ ¿se puede grabar, filmar o fotografiar?
- ❖ ¿Cómo consultar información complementaria?

Con este esquema, el perito se enfrenta a la escena del delito y debe exponer para el análisis del delito su experiencia que permitirá reconstruir el delito cometido, para ello puede considerar:

- ❖ ERR (esquema de reconstrucción relacional) indicios que evidencian correspondencia
- ❖ ERF (esquema de reconstrucción funcional) se explora cómo funcionan los elementos de análisis e inspección
- ❖ ERT (esquema o reconstrucción temporal) ubicación en la línea de tiempo y en directa relación con el evento destructivo.

Frente a la escena del delito que se explora o examina, el experto forense debe operar los referentes de seguimiento que se listan:

- ¿se empleó el sistema sin autorización o por fuera de lo acordado?
- ¿se obstaculizo o impidió el acceso normal a la red, al PC o a la información?
- ¿se borró, altero o estropeo sin orden o autorización del sistema?
- ¿se empleó software malicioso?
- ¿se violó la privacidad de la información y se distribuyó su contenido?
- ¿se generó un sitio web fantasma?
- ¿se actuó bajo la consigna del Ciberterrorismo digital?
- ¿existió la transferencia no consentida de activos o hubo algún hurto?
- ¿las consideraciones o estas preguntas presuponen entonces que el experto o perito en informática forense debe estar relacionado con este andamiaje jurídico: a9 Ley 527 de 1999: Comercio electrónico, b) Ley 599 de 2000: Violación de la comunicación, c) Ley 962 de 2005: Racionalización, d) Ley 1150 de 2007 Eficiencia y transparencia, e) Ley 1273 de 2009:Bien jurídico tutelado, e) Ley 1341 de 2009: Agencia Nacional del espectro, y f) Resolución 2258 de 2009: Seguridad en redes?

Convencionalmente, el experto debe acreditar el pleno dominio de las iniciativas formuladas por el CONPES 3701[14] que relacionan:

- Modelo de seguridad gobierno en línea
- Estrategia nacional de ciberseguridad
- Regulación del CSIRT-CCIT, centro de coordinación de atención a incidentes de seguridad informática.

[14] Consejo nacional de policita económica y social.
http://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Debiéndose tener presente, que el peritazgo informático a nivel forense, implica también por necesidad el tener presente lo establecido por los instrumentos jurisdiccionales en materia de ciberseguridad y ciberdefensa [Conpes 2010].

- Convenio sobre ciberseguridad de Budapest
- Resolución AG/RES 2004
- Decisión 587 comunidad andina
- Resolución 64/25 ONU[15]
- Conjunto de políticas a nivel mundial para impulsar la seguridad computacional o informática a saber: a) Estrategia de Seguridad Cibernética en Alemania 2011, b) Centro de operaciones cibernéticas. Australia 2010, c) Estrategia Cibernética de seguridad 2010 y e) Estrategia Internacional Para el Ciberespacio. USA 2011.

Como medio de recurrencia para efectos de interpretación en el entorno jurídico, se presenta como guía de formalización alusiva al tratamiento jurídico del delito informático en sentencia sp1245-2015 del 11 de febrero del 2015, promulgado por la corte suprema de justicia cuyo contenido se hace explícito en el anexo 2.

En resumen, el escenario generador de audiencias en el tratamiento del delito informático, producto de la construcción de solidas evidencias, quedo enunciado por [Conpes 2010]:

- Delitos bancarios: E-Banking
- Ciberbulling: acoso escolar

[15] Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional http://www.un.org/en/ga/search/view_doc.asp?symbol=A/64/PV.55&Lang=S

- Grooming: acoso sexual
- Sabotaje informático
- Lavado de dinero
- Pornografía
- Espionaje electrónico
- Piratería informática
- Robo de claves: Keylogging[16], Phishing[17] e ingeniería social[18]
- Robo de identidades

[16]Es un software o hardware que puede interceptar y guardar las pulsaciones realizadas en el teclado de un equipo que haya sido infectado http://www.segu-info.com.ar/malware/keylogger.htm

[17]Suplantación de identidad es un término informático http://seguridad.internautas.org/html/451.html

[18]Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

- Alteración firma electrónica
- Clonación tarjeta electrónica por uso de Skimmers [19]
- Falsificación de asientos controlados o tributarios

En el siguiente capítulo, se expondrá y desarrollara el andamiaje teórico y logístico del acopio de audiencia como base de soporte de la criminalística computacional.

[19]Duplica bandas magnéticas de tarjetas de crédito http://globbsecurity.com/lector-square-skimmer-clonar-tarjetas-35453/

3. CONTRUCCION DE LA SOLUCION

Este apartado, describe y formaliza la plataforma logística que enmarca en escenario de la criminalística computacional la construcción del modelo que regulara procedimentalmente la estructuración de evidencias como indicio o soporte probatorio para la tipificación del delito y posterior consideración legal por un juez de la república.

El marco descriptivo se fundamenta en la consideración y tratamiento de la criminalística digital o computacional, como el valorador o catalogador lógico que interpreta la fenomenología generada por la vulneración o perturbación de la confiabilidad, integridad y disponibilidad de un sistema Teleinformatico [Cano 2015], la inclusión de los términos valorador o catalogador lógico, presupone la interpretación sistémica que caracteriza a una disciplina de se desarrolla en un eje conceptual de mayor cobertura, en este caso la informática forense.
Se exponen secuencialmente, las temáticas asociadas con la tipología de evidencias, se formaliza la plataforma teórica del proceso de modelación, para operar el eje de referencia casuística de estudio y de esta forma proceder con la construcción del modelo.

3.1. ESCENARIO DE FOCALIZACION: EVIDENCIAS Y VULNERAVILIDADES

El experto en informática forense, para estructurar la manera integral el proceso de análisis de indicios y formulación de evidencias, debe estar relacionado con la valoración de vulnerabilidades en el sistema afectado [Bace 2000], estas vulnerabilidades se enmarcan en los siguientes ejes:

- Hardware
- Software
- Información
- Logística Operacional: a)Talento Usuario,

b)Infraestructura

Su integración, permite catalogar los referentes de acción que definen la casuística de ocurrencia [Rios 2004]; tal como se listan seguidamente:

- Políticas de seguridad: Diseño
- Puertas traseras: Implementación
- Mal uso del equipo: utilización equivocada
- Randomica o intencional: Día cero

En las figuras 19 (Diagrama sintáctico para vulnerabilidad básica), 20 (Diagrama sintáctico vulnerabilidad por referenciación) y 21 (Diagrama sintáctico vulnerabilidad generativa), se presenta el diagrama sintáctico que define la taxonomía de las vulnerabilidades de amplio espectro, dichas vulnerabilidades, se catalogan por segmentos de acción, a saber.

- Vulnerabilidad Básica: a)Validación, b)Salto, c)Seguimiento, d)Inyección sistema operativo
- Vulnerabilidad por referencia: a)Ejecución de script, b)Inyección SQL, c)Saturación de código, d)Saturación de espacio
- Vulnerabilidad generativa : a)Representación de datos, b)Filtrado, c)Autenticación o gestión de credenciales, d)Falencia criptográfica
- Vulnerabilidad de exploración: a)Incrustación de código en la web, b)Congelación por carrera, c)Saturación CPU, d)Propagación de Agujeros

Estas vulnerabilidades, expanden su efectividad en la llamada superficie de ataque [Rios 2004], la superficie de ataque, explicita funcionalmente los elementos siguientes:

- Arquitectura básica de computo
- Coherencia de gestión de archivos
- Patronato de enlace RPC
- Filtrado de intensificación
- Políticas de seguridad: a)Servicios, b)Mecanismos
- Expansión de tramas: a)Filtrado, b)Cobertura de protocolos, c)Segmentación tramas, d)Propagación DoS

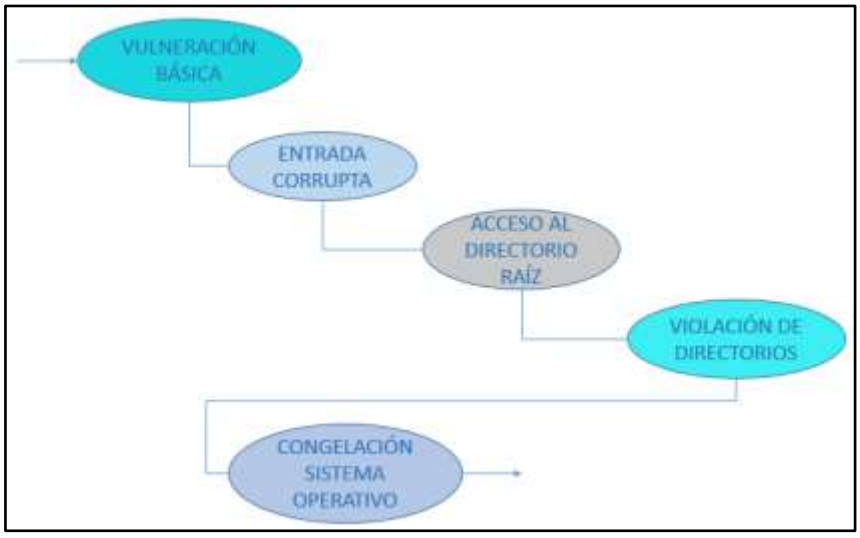


Figura 19: Diagrama sintáctico para vulnerabilidad básica

Fuente: Aporte realizadores

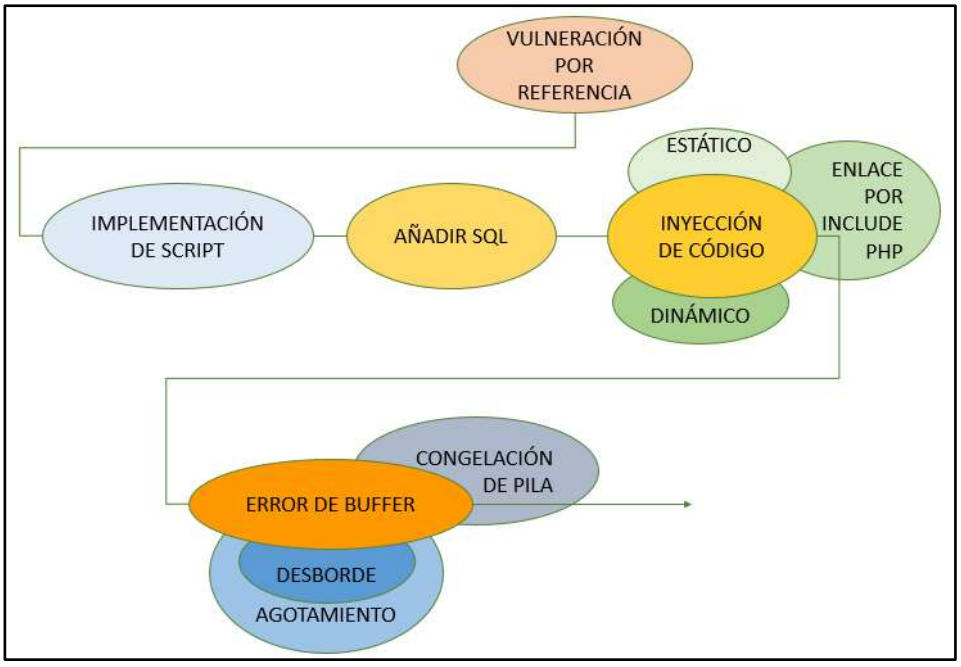


Figura 20: Diagrama sintáctico vulnerabilidad por referenciación

Fuente: Aporte realizadores colores

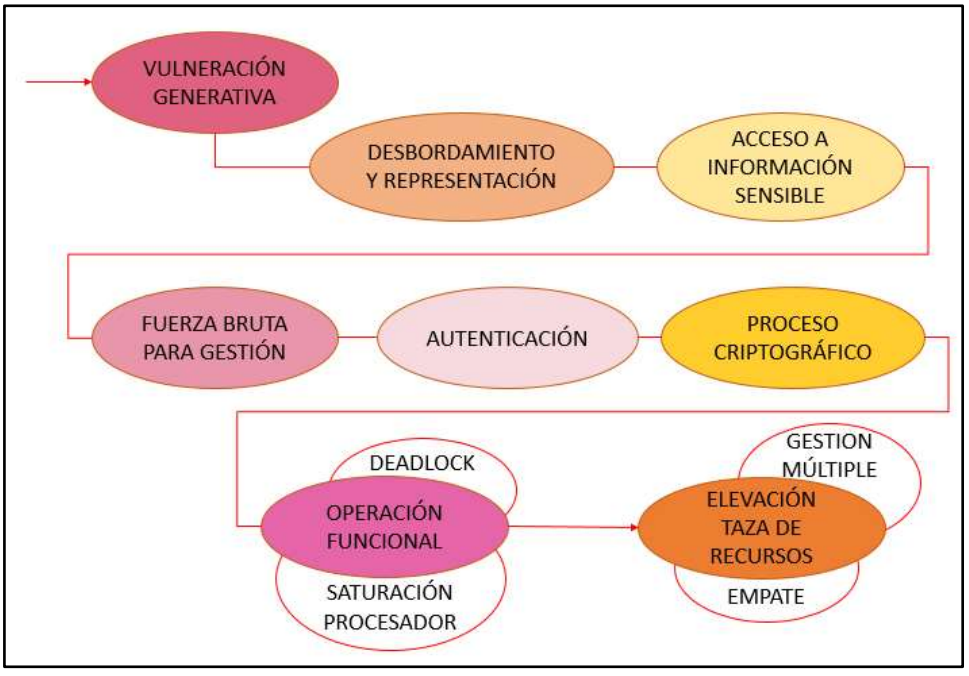


Figura 21: Diagrama sintáctico vulnerabilidad generativa

Fuente: Aporte realizadores

La visión formal para que el intruso de comienzo al proceso de exploración de vulnerabilidad, se define o estructura mediante el proceso de conocimiento del dominio, que fácilmente con ayuda del comando, whois.domaintools.com se puede obtener, por ejemplo al digitar http://whois.domaintools.com/unilibre.edu.co se obtiene esta instantánea que se lista ver figuras **22** (Instantánea Operacional De Dominio) **y 23** (Instantánea Operacional De Dominio II)

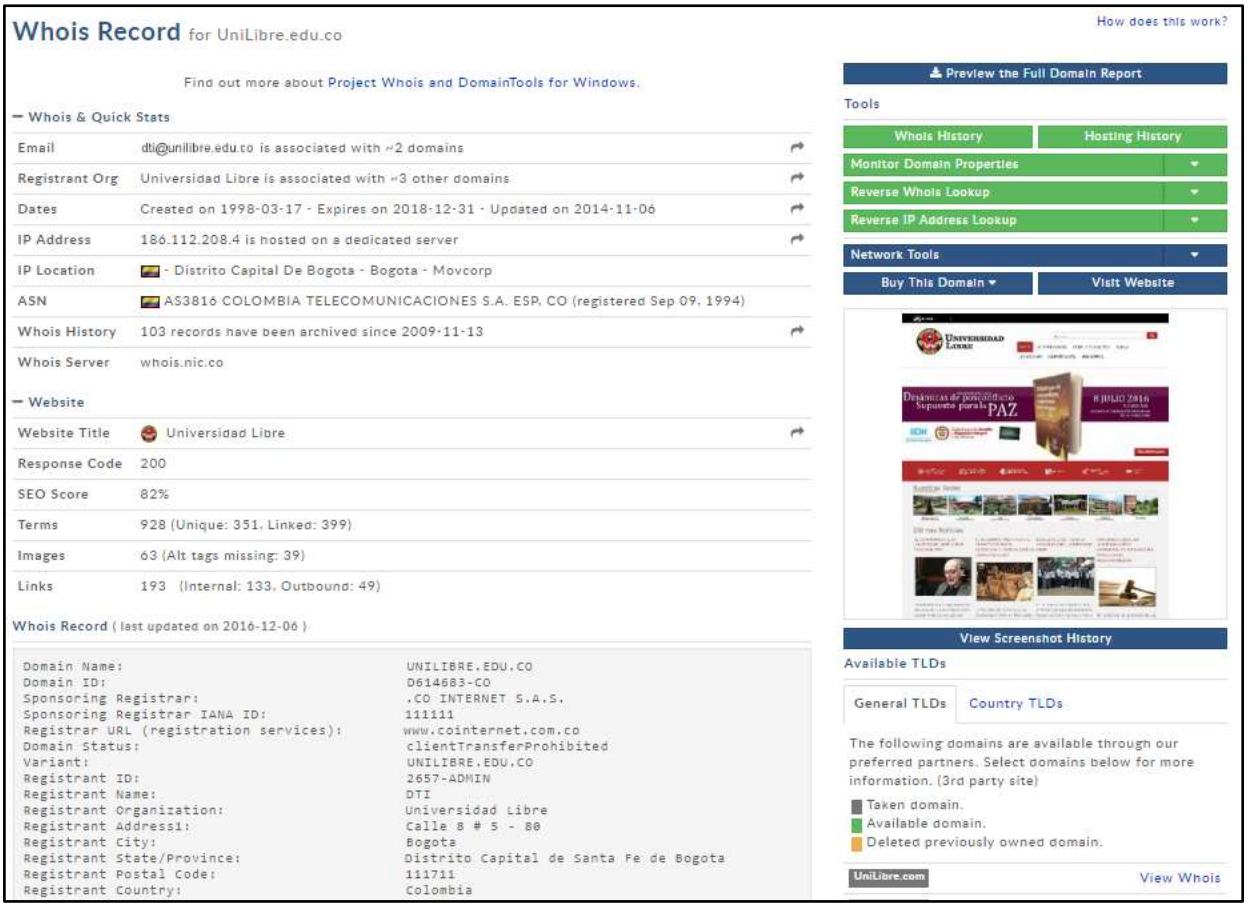
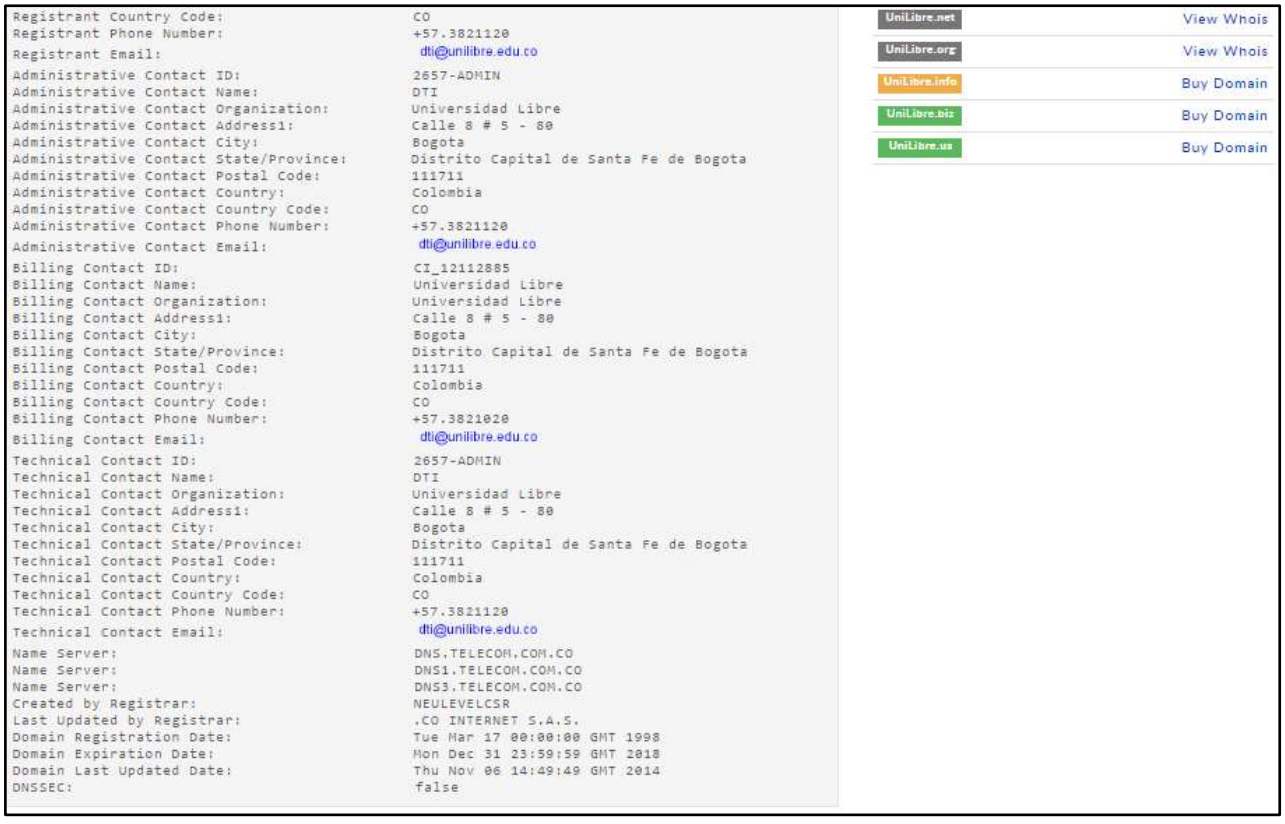


Figura 22: Instantánea Operacional De Dominio

Fuente: Aporte realizadores. Captura opción http://whois.domaintools.com/unilibre.edu.co



Registrant Country Code:	CO
Registrant Phone Number:	+57.3821120
Registrant Email:	dti@unilibre.edu.co
Administrative Contact ID:	2657-ADMIN
Administrative Contact Name:	DTI
Administrative Contact Organization:	Universidad Libre
Administrative Contact Address1:	Calle 8 # 5 - 80
Administrative Contact City:	Bogota
Administrative Contact State/Province:	Distrito Capital de Santa Fe de Bogota
Administrative Contact Postal Code:	111711
Administrative Contact Country:	Colombia
Administrative Contact Country Code:	CO
Administrative Contact Phone Number:	+57.3821120
Administrative Contact Email:	dti@unilibre.edu.co
Billing Contact ID:	CI_12112885
Billing Contact Name:	Universidad Libre
Billing Contact Organization:	Universidad Libre
Billing Contact Address1:	Calle 8 # 5 - 80
Billing Contact City:	Bogota
Billing Contact State/Province:	Distrito Capital de Santa Fe de Bogota
Billing Contact Postal Code:	111711
Billing Contact Country:	Colombia
Billing Contact Country Code:	CO
Billing Contact Phone Number:	+57.3821020
Billing Contact Email:	dti@unilibre.edu.co
Technical Contact ID:	2657-ADMIN
Technical Contact Name:	DTI
Technical Contact Organization:	Universidad Libre
Technical Contact Address1:	Calle 8 # 5 - 80
Technical Contact City:	Bogota
Technical Contact State/Province:	Distrito Capital de Santa Fe de Bogota
Technical Contact Postal Code:	111711
Technical Contact Country:	Colombia
Technical Contact Country Code:	CO
Technical Contact Phone Number:	+57.3821120
Technical Contact Email:	dti@unilibre.edu.co
Name Server:	DNS.TELECOM.COM.CO
Name Server:	DNS1.TELECOM.COM.CO
Name Server:	DNS3.TELECOM.COM.CO
Created by Registrar:	NEULEVELCSR
Last Updated by Registrar:	.CO INTERNET S.A.S.
Domain Registration Date:	Tue Mar 17 00:00:00 GMT 1998
Domain Expiration Date:	Mon Dec 31 23:59:59 GMT 2018
Domain Last Updated Date:	Thu Nov 06 14:49:49 GMT 2014
DNSSEC:	false

Figura 23: Instantánea Operacional De Dominio II

Fuente: Aporte realizadores. Tomado original opción http://whois.domaintools.com/unilibre.edu.co

Que puede completarse para su seguimiento con la ejecución del comando http://domainreport.domaintools.com/unilibre.edu.co para obtener el contenido mostrado en la figura 24

- Tendencia al desastre: a)Problemas ambientales, b)Ubicación de equipo, c)Potencia de UPS, d) No segmentación de cableado electrónico y cableado lógico
- Falencia logística: a)Economía y distribución de recursos equívocos, b)Carencia de políticas de seguridad, c)Talento humano ajeno al contexto tecnológico, d)Falta de capacitación ante la presencia de ataques, este último integra los siguientes núcleos diferenciadores, a saber:
    - Degeneración de servicio
    - Código malicioso
    - Accesos no autorizados
    - Fallas de conectividad

Seguidamente, se enuncian los factores o parámetros asociados con la definición de incoherencia o entropía estructural de un plan de seguridad: a) No se define ni los propósitos ni los objetivos, b)Se carece de un equipo para respuesta, c)No existen procedimientos de recuperación, d)No se conocen índices de vulneración, e) Se desconoce la fragilidad del sistema, para efectos de trazabilidad y seguimiento, acción que se obtiene mediante exploración del informe de errores.

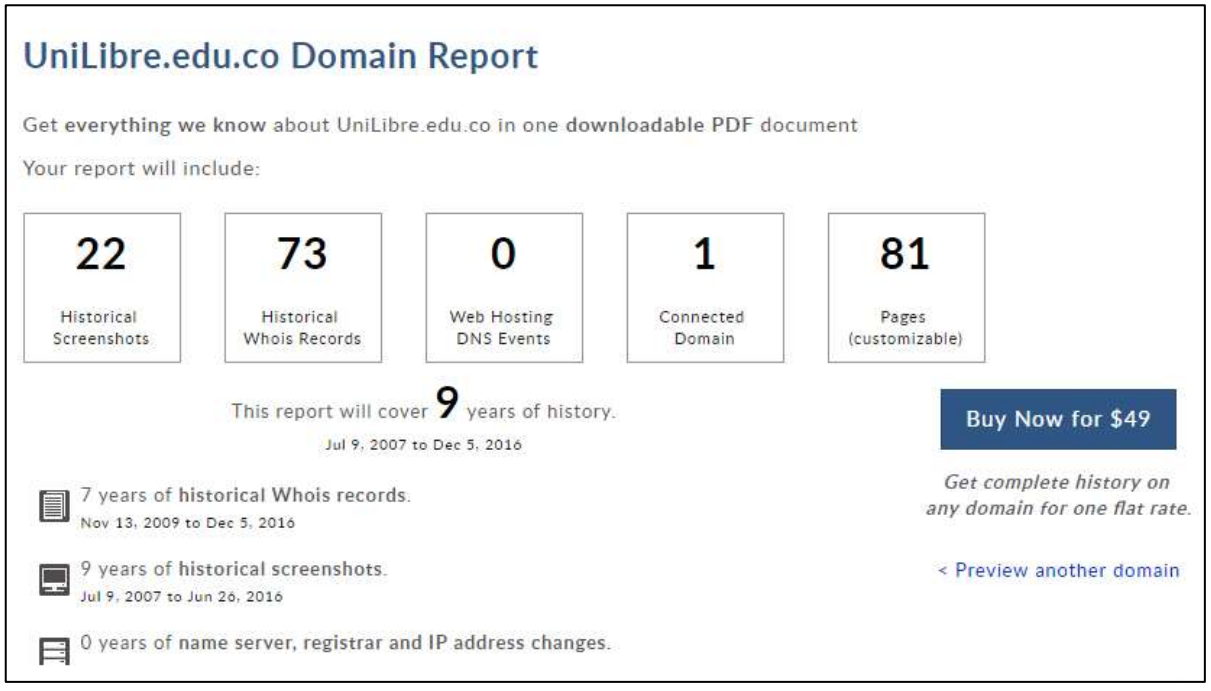


Figura 24: Instantánea Operacional De Dominio

Fuente: Aporte Realizadores. Captura Opción http://domainreport.domaintools.com/unilibre.edu.co

Este factor se visualiza con el acceso a MSINF032: informe de errores y allí se obtiene a nivel de ejemplo estas fichas de lectura o seguimiento:

28/11/2016 6:36 p.m. Windows Error Reporting Deposito con errores , tipo 0&#x000d ; &#x000a ; Nombre de evento: WindowsUpdateFailure3&#x000d ; &#x000a ; Respuesta: No disponible&#x000d ; &#x000a ; Identificador de archivo CAB: 0&#x000d ; &#x000a ; &#x000d ; &#x000a ; Firma del Problema: &#x000d ; &#x000a ; P1: 7.9.9600.18235&#x000d ;
 P2: 8024402c&#x000d ; &#x000a ; P3 00000000-0000-0000-0000-000000000000&#x000d ; &#x000a ; P4: Scan&#x000d ; &#x000a ; P5 0&#x000d ; &#x000a ; P6:1&#x000d ; &#x000a ; P7: 8024500b&#X000d ; &#x000a ; P8: AutomaticUpdates&#x000d ; &#x000a ; P9: {117CAB2D-

82B1-AB5A-A08C-4D62DBEE7782} &#x000d ; &#x000a ; P10: 0&#x000d ; &#x000a ; &#x000d ; &#x000a ; Archivos adjuntos:

 C:\WindowsUpdate.log&#x000d ; &#x000a ; C:\Windows\SoftwareDistribution\ReportingEvents.Log&#x000d ; &#x000a ; &#x000d ; &#x000a ; Es posible que estos archivos estén disponibles aquí: &#x000d ; &#x000a ; &#x000d ; &#x000a ; &#x000d ; &#x000a ; Simbolo de analisis: &#x000d ; &#x000a ; Nueva búsqueda de una solución: &#x000d ; &#x000a ; Identificador de Informe: 967f3b24-b599-11e5-8270-64006a6a7f39&#x000d ; &#x000a ; Estado del informe:262144&#x000d ; &#x000a ; Deposito de algoritmo hash:

28/11/2016 6:36 p.m. Windows Error Reporting Deposito con errores 125729805777, tipo 5&#x000d ; &#x000a ; Nombre de Evento: WindowsUpdateFailure3&#x000d ; &#x000a ; Respuesta: No disponible &#x000d ; &#x000a ; identificador de archivo CAB: 0&#x000d ; &#x000a ; &#x000d ; &#x000a ; Firma del problema: &#x000d ; &#x000a ; P1: 7.9.9600.18235&#x000d ; &#x000a ; P2: 8024402c&#x000d ; &#x000a ; P3: 00000000-0000-0000-0000-000000000000&#x000d ; &#x000a ; P4: Scan&#x000d ; &#x000a ; P5: 0&#x000d ; &#x000a ; P6: 1&#x000d ; &#x000a ; P7: 0&#x000d ; &#x000a ; P8: AutomaticUpdates&#x000d ; &#x000a ; P9: {3DA21691-E39D-4DA6-8A4B-B43877BCB1B7} &#x000d ; &#x000a ; P10: 0&#x000d ; &#x000a ; &#x000d ; &#x000a ; Archivos adjuntos: &#x000d ; &#x000a ; &#x000d ; &#x000a ; Es posible que estos archivos estén disponibles aquí: &#x000d ; &#x000a.

El desconocimiento de los índices de vulneración por parte del usuario ocasionan graves incidentes tanto de tipo económico como de malestar organizacional, por ejemplo mediante programación de tareas, se ejecuta el programa que se lista a continuación y no se tiene una respuesta oportuna, la pérdida de tiempo es creciente si el ataque se programa para que funcione cada vez que se reinicia el sistema; programa que se detendrá solamente si el usuario empieza a probar teclas y pulsa la correspondiente el SHIFT derecho, obviamente esto se logra cuando existen políticas de educación en el tema de la seguridad.

```
#include <windows.h>
#include <conio.h>
#include <stdlib.h>
#include <stdio.h>
```

```
#include <time.h>
Void unilibre (int a, int b)
{
    HANDLE libre;
    libre=GetStdHandle (STD_OUTPUT_HANDLE);
    COORD etm;
    etm.X=a;
    etm.Y=b;
    SetConsoleCursorPosition (libre.etm);
}
Main( )
{
  FreeConsole( );
  srand(GetTickCount( ))
  int v1 = GetSystemMetrics (SM_CXSCREEN) – 1;
  int v2 = GetSystemMetrics (SM_CYSCREEN) – 1;
  System (“color e2”);
  While (!GetAsyncKeyState (VK_RSHIFT));
    {
    unilibre((rand( ) % v1) + 5, (rand( ) % v2) + 5));
    printf (“Universidad libre 2016\n”);
    Sleep (5);
    system (“cls”);
    system (“color a3”);
    Printf(“Ingenieria de Sistemas○\n”);
    Sleep (3);
    printf(“Gracias por utilizar nuestros servicios\n”);
    Sleep (500);
        system (“color d5”);
          system (“cls”);
    system (“color a3”);
```

```
    printf("Jennifer y Pavel, programa perturbador 05/12/2016";
    Sleep(3);
    }
  System("narrator");
  Return (0);
}
```

Tomando como núcleo de observación el contenido presentado, es necesario que el experto o perito en informática forense durante el proceso de estructuración de evidencias pueda sondear al talento humano responsable del equipo afectado, para ello debe conocer con propiedad la fundamentación relacionada con el andamiaje piramidal de observación y configuración de seguridad [Stallings 2012], para ello los factores básicos y preponderantes de recurrencia: se muestran como guía para formulación de las preguntas de acopio del acceso para configurar la evidencia a saber:

- ¿Los programas de cargue del sistema han sido modificados?
- ¿Las firma digitales del software de control de validad contundente?
- ¿Los mecanismos de protección del sistema a nivel de usuario se revisan diariamente?
- ¿Cada conjunto se evalúa el IOELOG del sistema?
- ¿La caída o desconexión de la red es usual, periódica o nunca ocurre?
- ¿Conoce cómo funciona el KDC[20] (Key Distribution Center) y el FEP[21] (Frond End Processor)?
- ¿Cuál es la base lógica para el intercambio de autentificación cliente /servidor?
- ¿Las políticas de seguridad son reflejo directo de X.509?
- ¿Se conoce e implementa el campo de confianza en el manejo de claves?
- ¿Se ha determinado con la práctica la plataforma de seguridad avanzada en el manejo de correo electrónico a nivel de estos servicios: recibos firmados, etiquetas se seguridad, listas de correo?

[20] Es parte de un sistema de cifrado destinado a reducir los riesgos inherentes en el intercambio de claves. Los KDC a menudo operan en sistemas dentro de los cuales algunos usuarios pueden tener permiso para usar ciertos servicios en algunas ocasiones y no en otros http://directory.apache.org/apacheds/kerberos-ug/1.1.4-kdc.html

[21] Proceso de comunicación es un pequeño computador el cual sirve como interfaz entre un computador host y un número de redes, como una SNA o un número de dispositivos periféricos, como terminales, unidades de disco, impresoras y unidades de cinta. http://www.osii.com/pdf/scada-ui/openfep_ps.pdf

- ¿Conoce la codificación del certificado a nivel de carga útil: Hash, Firma, Nonce, Notificación?
- ¿En el tratamiento de integridad, confidencialidad, denegación y autenticación que amenazas han registrado?
- Está familiarizado con el sistema SET: a)Titular, b)Vendedor, c)Emisor, d)Adquisidor, e)Pasarela de pago, f)Autoridad de certificación
- ¿Ha evaluado la funcionalidad de la configuración del agente proxy?
- ¿Sabe algo sobre motores autoritativos y no autoritativos?
- ¿Las políticas de seguridad incluyen en el control de acceso basado en vistas (VACM)[22]?

El perito forense, debe estar completamente familiarizado con estos factores fundamentales que aluden al proceso de detección de intrusos a saber [Mchugh 2000]:

- Detección basada en reglas
- Nivel de tasa de sospecha
- Falencia de la tasa de base
- Detección distribuida:
  - Control modulo agente del Host
  - Control agente monitor
  - Control administrador central
  - Implementación de

[22] Describe el modelo de control de acceso basado en Vista para su uso en la arquitectura SNMP. Define los Elementos de Procedimiento para controlar el acceso a la información de gestión. https://www.webnms.com/cagent/c_snmp_agent_datasheet.html

Honeypots
- Controlador de contraseñas proactivo
- Enlace y acceso a las tablas de Hash
- Técnicas de Ransomware[23]

❖ Seguimiento matemático e interpretación de la significación del flujo de tareas, por validación de la cola de recepción y disponibilidad del sistema (Prawda 2012)

$$\boldsymbol{Disponibilidad}\ P = \frac{\lambda}{\mu} \quad (1)$$

$$\boldsymbol{Probabilidad\ servidor\ vacío}\ Po(t) = 1 - \frac{\lambda}{\mu} \quad (2)$$

$$Pk\ (t) = \left(\frac{\lambda}{\mu}\right)^{K} Po\ (t)\ Probabilidad\ de\ antender\ (K-2)\ usuario\ teniendo\ K\ en\ cola$$

(3)

[23] Del inglés Ransom, 'rescate', y Ware, por software) es un tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción. http://www.trendmicro.com/vinfo/us/security/definition/Ransomware

$$\textbf{Longitud de la cola: } L = \frac{\lambda^2}{\mu\,(\mu - \lambda)} \quad (4)$$

$$\textbf{Longitud del sistema: } W = \frac{\lambda}{\mu - \lambda} \quad (5)$$

$$\textbf{Tiempo de permanencia del usuario en la cola: } Tq = \frac{\lambda}{\mu\,(\mu - \lambda)} \quad (6)$$

$$\textbf{Tiempo de permanencia en el sistema: } Tw = TS + \frac{1}{\mu} \quad (7)$$

Probabilidad de existir más de K transacciones: $P\,(W > K) = \rho^{k+1}$ (8)

$$\textbf{Probabilidad de demora de K unidades de la cola: } \text{P (Tq>K)} = \frac{\lambda}{\mu} e^{-\mu(1-\frac{\lambda}{\mu})t} \quad (9)$$

- Operaciones Buhtrap[24]
  - Mensaje de spam
  - Se abre el archivo malicioso
  - Se encadena servidor externo
  - Se accede remotamente al control
- Set de ataques APT[25] (Advanced Persistent Threat)
- Ecosistemas y Crimeware[26]
- Tendencias a la Haxposicion[27]
- Impacto del malware en equipos moviles

[24] Buhtra proviene de la mezcla de dos palabras: "Buhgalter" y "trap". "Buhgalter" significa "contador" en ruso y "trap" es "trampa" en inglés. http://www.welivesecurity.com/la-es/2015/04/09/operacion-buhtrap/

[25] Es un conjunto de procesos informáticos sigilosos y continuos, a menudo orquestados por humanos, dirigidos a penetrar la seguridad informática de una entidad específica. http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT

[26] Tipo de software utilizado por los atacantes o intrusos para activar operaciones ilícitas en el entorno financiero con presencia virtual del dueño de las transacción http://www.webantivirus.com.ar/prevencion-de-amenazas/amenazas-mas-comunes/crimeware.html

[27] Surge de la combinación de dos clásicos: hacking y exposición de datos. Hace referencia, entonces, al robo de datos mediante ataques informáticos y la consecuente divulgación pública. http://www.systec.co.cr/sabes-que-es-la-haxposicion-conoce-a-esta-amenaza-emergente/

- Empleo de SCADA[28] (Supervisory Control And Data Acquisition)
- Envio de Sexting[29] o contenidos eróticos
- Empleo del ciberbullying[30]
- Diestro manejo de ISO/IEC 2700[31]

Básicamente, según ocurrencia genérica de los ataques informáticos, se resume en la figura 25, el índice y frecuencia de acopio de las evidencias que el perito forense presenta para sustentación del delito cometido.

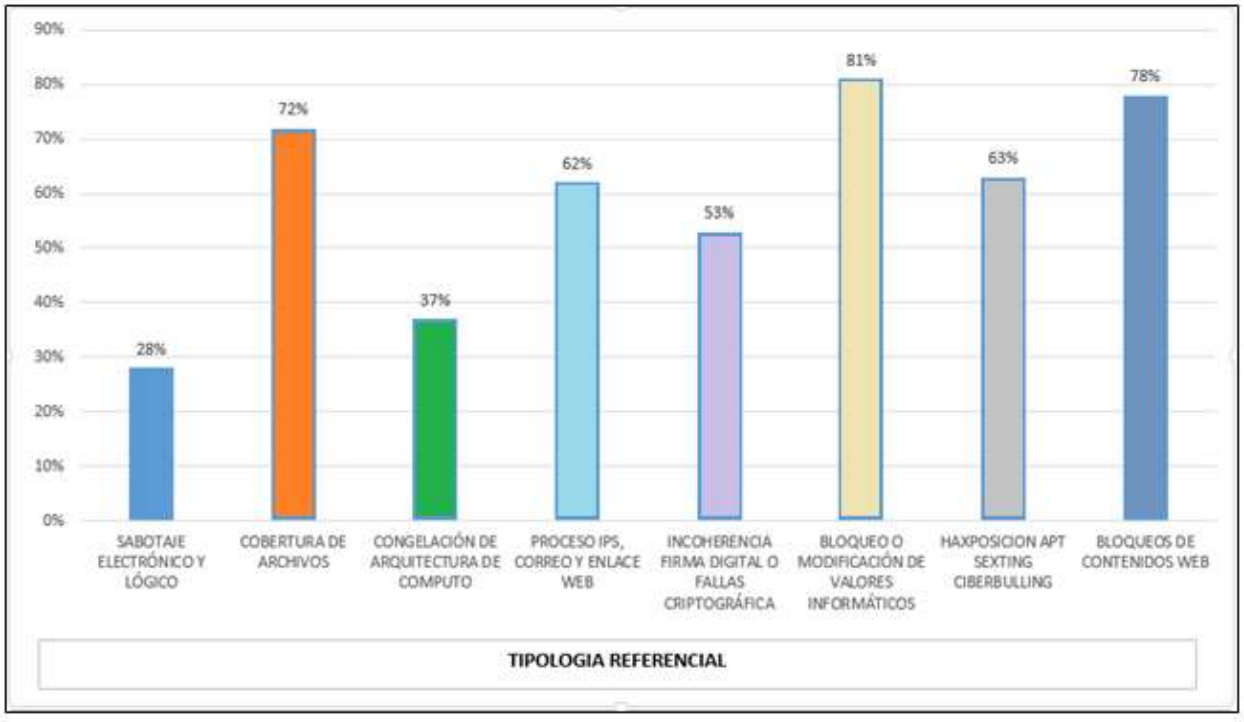


Figura 25: Índice Escenario Generador De Evidencias.

Fuente: Aporte realizadores. Consulta ESET (Enjoy Safer Technology)

[28] (Supervisión, Control y Adquisición de Datos) es un concepto que se emplea para realizar un software para ordenadores que permite controlar y supervisar procesos industriales a distancia. http://www.uco.es/investiga/grupos/eatco/automatica/ihm/descargar/scada.pdf

[29] Término en inglés que se usa para referirse al acto de enviar mensajes (SMS o MMS) explícitos de contenido erótico o sexual desde un dispositivo móvil. http://www.sexting.es/que-es-el-sexting/

[30] Medio o táctica de despliegue de interacción teleinformática con la que se acosa, molesta o distorsiona la labor o rutina formal de un usuario declarado como objetivo del ataque. http://www.ciberbullying.com/cyberbullying/que-es-el-ciberbullying/

[31] Serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC). http://www.iso27000.es/download/doc_iso27000_all.pdf

Con ayuda de la figura anterior, es fácil confirmar como el proceso de elaboración de evidencias, exige al perito o experto en informática forense, el poseer una sólida fundamentación en el mapeo operacional de la arquitectura computacional, como ejemplo se cita el uso adecuado del comando WMIC, para evaluar las características de procesador: **wmic/output:stdout cpu get/all/format:list**

Que genera estos parámetros:

AddressWidth=32
Architecture=9
Availability=3
Caption=x64 Family 6 Model 60 Stepping 3
ConfigManagerErrorCode=
ConfigManagerUserConfig=
CpuStatus=1
CreationClassName=Win32_Processor
CurrentClockSpeed=3600
CurrentVoltage=12
DataWidth=64
Description=x64 Family 6 Model 60 Stepping 3
DeviceID=CPU0
ErrorCleared=
ErrorDescription=
ExtClock=100
Family=206
InstallDate=
L2CacheSize=512
L2CacheSpeed=
L3CacheSize=3072
L3CacheSpeed=0
LastErrorCode=
Level=6

LoadPercentage=14

Manufacturer=GenuineIntel

MaxClockSpeed=3600

Name=Intel(R) Core(TM) i3-4160 CPU @ 3.60GHz

NumberOfCores=2

NumberOfLogicalProcessors=4

OtherFamilyDescription=

PNPDeviceID=

PowerManagementCapabilities=

PowerManagementSupported=FALSE

ProcessorId=BFEBFBFF000306C3

ProcessorType=3

Revision=15363

Role=CPU

SocketDesignation=SOCKET 0

Status=OK

StatusInfo=3

Stepping=

SystemCreationClassName=Win32_ComputerSystem

SystemName=BOGADMA674SUP01

UniqueId=

UpgradeMethod=36

Version=

VoltageCaps=

De igual forma se puede obtener información sobre:

- Redes: nicconfig
- Servicios: service
- Memoria: memphisical
- Programas de inicio: startup

- Puntos de conexión: system lot
- Información servidor: server
- Termometro electrónico: temperature
- Voltaje: voltaje
- Gestión remota: rdaccount
- Información chip de memoria: memorychip

Al ejecutar por ejemplo el comando: **wmic /output:stdout netlogin get /all /format:list**

Se obtiene la información asociada el nombre, nombre completo, ScriptPath, Perfil, ID de usuario, NumberOfLogons, PasswordAge, logonserver, sea homeDirectory, PrimaryGroupID

Profile=
ScriptPath=
SettingID=
UnitsPerWeek=
UserComment=
UserId=
UserType=
Workstations=

AccountExpires=
AuthorizationFlags=
BadPasswordCount=
Caption=NT AUTHORITY\SERVICIO LOCAL
CodePage=
Comment=
CountryCode=
Description=Network login profile settings for SERVICIO LOCAL on NT AUTHORITY
Flags=

FullName=

HomeDirectory=

HomeDirectoryDrive=

LastLogoff=

LastLogon=

LogonHours=

LogonServer=

MaximumStorage=

Name=NT AUTHORITY\SERVICIO LOCAL

NumberOfLogons=

Parameters=

PasswordAge=

PasswordExpires=

PrimaryGroupId=

Privileges=

Profile=

ScriptPath=

SettingID=

UnitsPerWeek=

UserComment=

UserId=

UserType=

Workstations=

AccountExpires=

AuthorizationFlags=

BadPasswordCount=

Caption=NT AUTHORITY\Servicio de red

CodePage=

Comment=

CountryCode=

Description=Network login profile settings for Servicio de red on NT AUTHORITY

Flags=

FullName=

HomeDirectory=

HomeDirectoryDrive=

LastLogoff=

LastLogon=

LogonHours=

LogonServer=

MaximumStorage=

Name=NT AUTHORITY\Servicio de red

NumberOfLogons=

Parameters=

PasswordAge=

PasswordExpires=

PrimaryGroupId=

Privileges=

Profile=

ScriptPath=

SettingID=

UnitsPerWeek=

UserComment=

UserId=

UserType=

Workstations=

AccountExpires=

AuthorizationFlags=0

BadPasswordCount=0

Caption=FidelRR

CodePage=0

Comment=Profesional de Procesos

CountryCode=170

Description=Network login profile settings for Fidel Mauricio Rodriguez Realpe o

n SALUDTOTAL

Flags=513

FullName=Fidel Mauricio Rodriguez Realpe

HomeDirectory=

HomeDirectoryDrive=

LastLogoff=**********.******+***

LastLogon=20161207132836.000000-300

LogonHours=Sunday: No Limit -- Monday: No Limit -- Tuesday: No Limit -- Wednesda

y: No Limit -- Thursday: No Limit -- Friday: No Limit -- Saturday: No Limit

LogonServer=*

MaximumStorage=4294967295

Name=SALUDTOTAL\FidelRR

NumberOfLogons=6376

Parameters=

PasswordAge=00000029070845.000000:000

PasswordExpires=20161223091422.000000-300

PrimaryGroupId=513

Privileges=1

Profile=

ScriptPath=restusb.vbs

SettingID=

UnitsPerWeek=168

UserComment=BlmuNmW8QzbIP1urlYH2q9/zqAmVhShb6U6oro1UjMZxm/vY0sj+gDau5iwZw

QkiFN5W

ckJoheAn+lDYTEtOhFaTEIMcozyrmtDS5/IXmQERMQbooSCojKG4w38yeAs7/7sea/kR4a9tbbh

HHUZH

qNZ3JRpsVAN00LDpFJ7sr5bgy1adVHIxllZIinbun7vPHp3WQ/UFSMderyQwSeBzMlNaXJgxRf
BV
UserId=137040
UserType=Normal Account
Workstations=

AccountExpires=
AuthorizationFlags=0
BadPasswordCount=0
Caption=SergioGoC
CodePage=0
Comment=Field Services Representative I
CountryCode=170
Description=Network login profile settings for Sergio Yeloan Gonzalez Cagua on S
ALUDTOTAL
Flags=513
FullName=Sergio Yeloan Gonzalez Cagua
HomeDirectory=
HomeDirectoryDrive=
LastLogoff=**********.******+***
LastLogon=20161205120532.000000-300
LogonHours=Sunday: No Limit -- Monday: No Limit -- Tuesday: No Limit -- Wednesda
y: No Limit -- Thursday: No Limit -- Friday: No Limit -- Saturday: No Limit
LogonServer=*
MaximumStorage=4294967295
Name=SALUDTOTAL\SergioGoC
NumberOfLogons=1971
Parameters=
PasswordAge=00000042072228.000000:000
PasswordExpires=20161210090040.000000-300

PrimaryGroupId=513
Privileges=1
Profile=
ScriptPath=habusb.vbs
SettingID=
UnitsPerWeek=168
UserComment=
UserId=138893
UserType=Normal Account
Workstations=

AccountExpires=
AuthorizationFlags=0
BadPasswordCount=0
Caption=GermanAR
CodePage=0
Comment=Subdirector Nacional de Conciliaciones
CountryCode=170
Description=Network login profile settings for German Dario Amortegui Rodriguez
on SALUDTOTAL
Flags=513
FullName=German Dario Amortegui Rodriguez
HomeDirectory=\\srvapimg\Vicepresidencias
HomeDirectoryDrive=M:
LastLogoff=**********.******+***
LastLogon=20161207140415.000000-300
LogonHours=Sunday: No Limit -- Monday: No Limit -- Tuesday: No Limit -- Wednesda
y: No Limit -- Thursday: No Limit -- Friday: No Limit -- Saturday: No Limit
LogonServer=*
MaximumStorage=4294967295

Name=SALUDTOTAL\GermanAR
NumberOfLogons=203
Parameters=
PasswordAge=00000025233138.000000:000
PasswordExpires=20161226165132.000000-300
PrimaryGroupId=513
Privileges=1
Profile=
ScriptPath=habusb.vbs

AccountExpires=
AuthorizationFlags=0
BadPasswordCount=0
Caption=EnriqueRC
CodePage=0
Comment=Supervisor de Operaciones en Salud - Conciliaciones
CountryCode=170
Description=Network login profile settings for Pavel Enrique Ramirez Castillo on
SALUDTOTAL
Flags=513
FullName=Pavel Enrique Ramirez Castillo
HomeDirectory=
HomeDirectoryDrive=
LastLogoff=**********.******+***
LastLogon=20161205094631.000000-300
LogonHours=Sunday: No Limit -- Monday: No Limit -- Tuesday: No Limit -- Wednesda
y: No Limit -- Thursday: No Limit -- Friday: No Limit -- Saturday: No Limit
LogonServer=*
MaximumStorage=4294967295
Name=SALUDTOTAL\EnriqueRC
NumberOfLogons=277

Parameters=

PasswordAge=00000004232608.000000:000

PasswordExpires=20170116165702.000000-300

PrimaryGroupId=513

Privileges=1

Profile=

ScriptPath=restusb.vbs

SettingID=

UnitsPerWeek=168

UserComment=/9txh8QXiPU5vnu7PiitmjgA45ANk3aAojoCLOo3gdEcMI/qDcdKYQ==

UserId=67396

UserType=Normal Account

Workstations=

AccountExpires=

AuthorizationFlags=0

BadPasswordCount=0

Caption=soporte

CodePage=0

Comment=

CountryCode=0

Description=Network login profile settings for on BOGADMA674SUP01

Flags=66081

FullName=

HomeDirectory=

HomeDirectoryDrive=

LastLogoff=**********.******+***

LastLogon=20151027172301.000000-300

LogonHours=Sunday: No Limit -- Monday: No Limit -- Tuesday: No Limit -- Wednesda

y: No Limit -- Thursday: No Limit -- Friday: No Limit -- Saturday: No Limit

LogonServer=*
MaximumStorage=4294967295
Name=BOGADMA674SUP01\soporte
NumberOfLogons=12
Parameters=
PasswordAge=00000417100456.000000:000
PasswordExpires=
PrimaryGroupId=513
Privileges=2
Profile=
ScriptPath=
SettingID=
UnitsPerWeek=168
UserComment=
UserId=1002
UserType=Normal Account
Workstations=

Parameters=
PasswordAge=00000001065123.000000:000
PasswordExpires=
PrimaryGroupId=513
Privileges=2
Profile=
ScriptPath=
SettingID=
UnitsPerWeek=168
UserComment=
UserId=500
UserType=Normal Account
Workstations=

3.2. CRIMINALISTICA DIGITAL: ASPECTOS LOGICOS PARA MAPEO DE EVIDENCIAS

Pretender definir que es la criminalística digital, sin sustentar su alcance o cobertura en el ámbito forense, resulta algo muy complicado, pues como se sabe jurídicamente la criminalística es la disciplina del pequeño detalle [Osterburg 2000], quien la define como el conjunto de conocimientos que tiene por finalidad determinar, desde el enfoque pericial que se cometió un delito, señalando el responsable y explicando el cómo se llevó a cabo. El soporte de la criminalística, se encuentra en estos focos disciplinares, a saber:

- Arte Forense: Construye la imagen o retrato hablado
- Antropología Forense: Reconstrucción del cadáver y determinación de sexo, edad, talla y raza
- Balística Forense: Estudio físico de los instrumentos empleados
- Dactiloscopia: Impresión Dactilar
- Documentoscopia[32]: estudio de referencias escitas para ampliar la visión de la investigación
- Entomología: Análisis de artrópodos que llevan el cadáver
- Fisionomía: Reconstrucción del rostro
- Fotografía: Mapeo geométrico del área de ataque donde se cometió la acción
- Genética: Estudio Biológico
- Análisis Químico: Valoración química del entorno
- Hematología: Análisis manchas e sangre
- Necrocomia: Estudio del cadáver
- Meteorología: Condiciones climáticas
- Caligrafía: Autenticidad de documentos

[32] Termino derivado del vocablo latino documentor (que enseña y muestra) y del termino girego Skopein (ver u observar) http://www.policia.gob.ni/cedoc/_private/lev2

- Disciplinas complementarias: a)Piloscopia[33], b)Psicología Forense[34], c)Química Forense[35], d)Toxicología Forense

La acción de experto en criminalística se resume en la integración de los procesos que se listan [Nachenberg 2003]:

- Protección del lugar de los hechos
- Valoración espacial del lugar
- Evaluación y fijación
- Levantamiento de indicios
- Cotejamiento en el laboratorio
- Cadena de custodia
- Elaboración de informe pericial

La figura 26 señala el esquema de acción procedimental de la criminalística forense; las acciones o fases mostradas, presupone la incorporación de un investigador responsable de: a)Orientación procedimientos técnicos, b)estructura esquemas operativos, c)Establecer procedimientos científicos según lo establecido en el sistema penal acusatorio colombiano; perfil que puede desarrollarse en estos escenarios:

- Policía Judicial
- Asesor técnico en entidades del sector público y privado
- Asesor fuerzas de seguridad
- Valorador de incidentes o atentados contra la seguridad

[33]Es la parte de la medicina forense que se encarga del estudio del pelo. https://issuu.com/danielsanchezvargas16/docs/libro-criminalistica

[34]Es la disciplina originada en la psicología clínica, resultado de la necesidad de una evaluación psicológica de la criminalidad, y que es producto de la unión de la psicología con el derecho. http://www.apuntesdepsicologia.com/ramas-de-la-psicologia/psicologia-forense.php

[35]Rama de la química que estudia las interacciones entre compuestos de naturaleza orgánica e inorgánica existentes en la escena de un crimen como pigmentos, trozos de tela, vidrio, restos de objetos de arte, pólvora, sangre y tejidos, entre otros, y tiene como objetivo el contribuir desde el punto de vista científico al esclarecimiento o resolución de hechos delictivos. http://www.estudiocriminal.eu/media/Quimica%20Forense%20Quimica%20Analitica%20Aplicada%20a%20la%20Criminologia.pdf

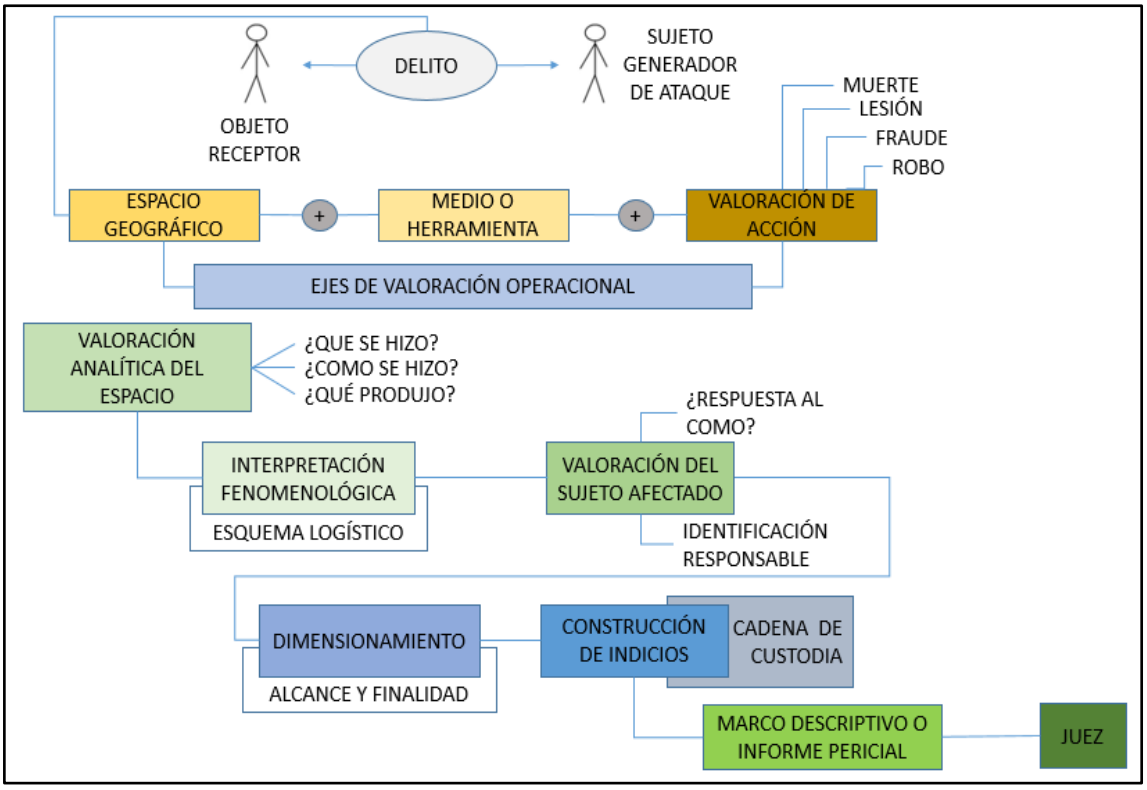


Figura 26: Esquema Procedimental De Criminalística

Fuente: Aporte realizadores

3.2.1. LEXICO DEL ESCENARIO CRIMINALISTICO

Tal como se señaló en la figura 26, la procedencia de los tres segmentos o niveles, determina el conocimiento de los conceptos de operación que relacionan los ejes de valoración, la logística sistémica y la mecánica instrumental del investigador, cada una de las cuales se define aquí:

3.2.1.1. EJE DE VALORACION OPERACIONAL

Contextualiza el escenario donde se aplica el ataque, para valorar la casuística que se presenta y estudia a la luz de la tecnología, los ejes o focos de análisis para el experto o perito forense.

- Destrucción de archivos
- Modificación de contenidos
- Fragmentación IP
- Desbordamiento
- Denegación de servicio
- Desactivación del filtro MAC
- Suplantación de ARP

- Validación de Agentes: a)Phishing, b)Ransomware, c)Roque Dialer, d)Click - Jacking[36], e)RFI (Remote File Inclusion), f)Ghost Domain[37] y g)Valoración de Diodos como supresores
- Dimensionamiento de seguridad perimetral: a)Perimetral Abierto, b)Perimetral Cerrado, c)Firewall y d)VPN
- Nivel de Conectividad: a)VPN Router – Router, b)VPN Firewall – Firewall
- Catalogación Funcional: a)Autenticidad, b)Integridad y c)Disponibilidad
- Técnicas de reconocimiento: a)Google Hacking, b)Ingeniería Social y c)Sniffing

3.2.1.2. EJE DE LOGISTICA FUNCIONAL

Valida los considerandos de interpretación legal, al evaluar el daño ocasionado e identificar frente a la normativa legal el incidente que se evalúan o analiza a saber:

- Interrupción del sistema
- Acceso abusivo
- Interceptación
- Daño Informático
- Uso software malicioso
- Violación datos personales
- Suplantación sitios WEB

3.2.1.3. EJE PARCIAL

Dimensiona, construye estipula los parámetros de la cadena de custodia, determinando:

- Potencialidad destructiva
- Plan de recuperación
- Valoración económica del impacto
- Estrategia de seguimiento al intruso
- Elaboración de indicio

[36] Técnica utilizada por los hackers para capturar información confidencial o asumir el control de la estación al pulsar el despliegue de una página web de manera transparente. http://web.archive.org/web/20160909181944/http://www.sectheory.com/clickjacking.htm

[37] Dominio fantasma o sitio WEB inexistente que camufla una operación indebida para sustracción indebida o toma de control de la estación por parte del Hacker http://www.ntn24.com/noticia/cuidado-expertos-alertan-sobre-un-dominio-falso-que-es-similar-a-google-y-podria-danar-su-equipo-124342

- Refinamiento de evidencia
- Formalización cadena de custodia
- Estructuración judicial

3.2.2. PATRONATO REFERENCIAL DE EVIDENCIA

Siendo la evidencia el núcleo de representación formal de la tecnología de la criminalística digital, se hace necesario considerar los núcleos operativos que validan tanto el vector de ataque como el impacto destructivo que permitirá generar la evidencia, por ejemplo el experto en informática forense, que se enfrenta a un ataque de denegación de servicio, deberá considerar el patronato señalado en la figura 27. [Garcia 2013], para dimensionar el condicionamiento de carácter legal que ha de trabajarse:

- IPFLOODING: Inundación Masiva de la red por Datagramas IP
- SMURF: Suplantación de direcciones de Origen y destino
- TCP/SYN FLOODING: Activación de conexiones para configurar la inundación
- TEARDROP: utilización fraudulenta de fragmentación IP para confundir el sistema
- SNORK: Utilización malintencionada de servicios
- PING OF DEATH: Ping o barrido de la muerte
- ATAQUE DISTRIBUIDO: Múltiples equipos para atacar un mismo objetivo
  - TRINOO
  - TFN (Tribe Flood Network)
  - SHAFT
  - TRIBE FLOOD NETWORK 2000

El despliegue del patronato formal de la evidencia, en el entorno de la auditoría y control, determina [Brings 2003].

3.2.2.1. VALORACIÓN DE CARACTERÍSTICAS

Determina la confiabilidad y valor agregado del indicio que se evalúa, debiéndose considerar; estos aspectos:

- Relevancia
- Autenticidad
- Verificabilidad

- ❖ Neutralidad
- ❖ Riesgo inherente
- ❖ Riesgo de control
- ❖ Prueba de control

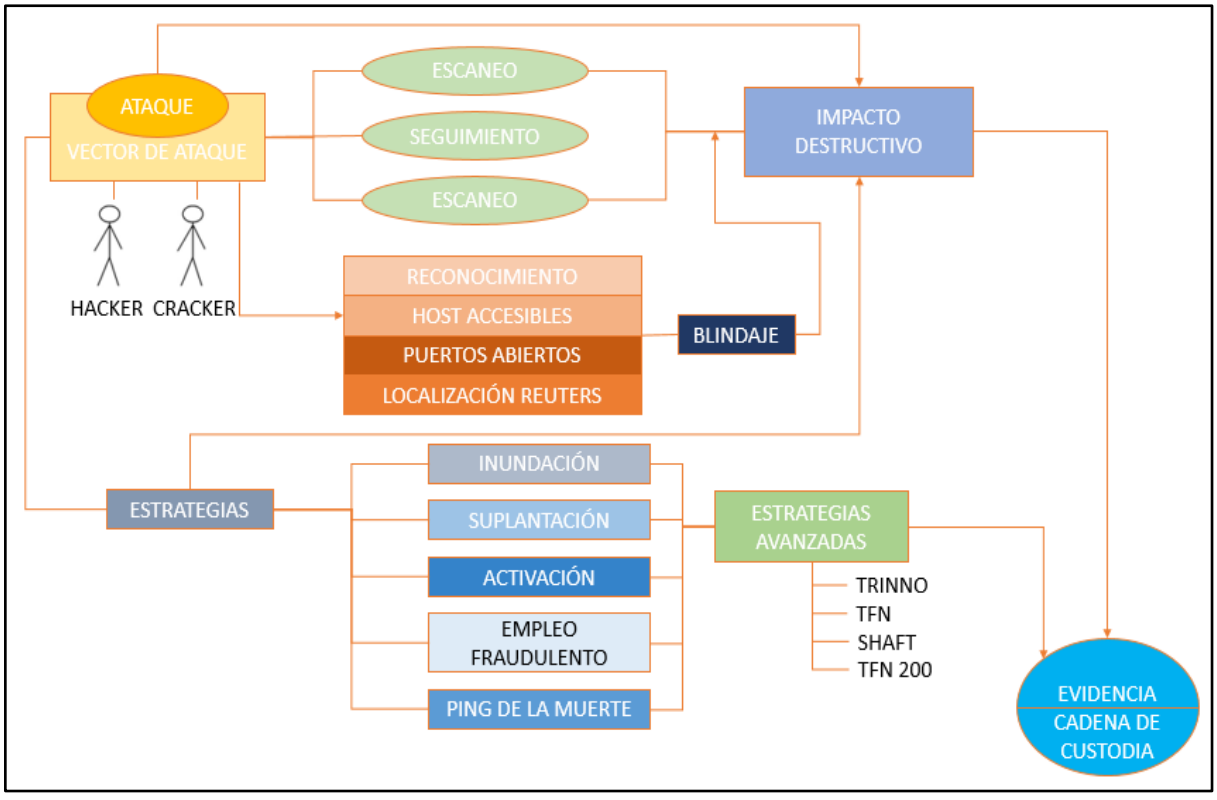


Figura 27: Patronato Condicionado de Evidencia

Fuente: Aporte realizadores

3.2.2.2. TECNICA PROCEDIMENTAL

Método empleado para validar la legitimidad de la información que genera el indicio considerado, está conformado por:

- ❖ Mecánica de inspección
  - o Documental
  - o Físico
    - ✓ Conectividad
    - ✓ Arquitectura de computo
    - ✓ Arquitectura telemática

- ❖ Observación
  - o Valoración geométrica y física del medio
  - o Indagación Explicativa
  - o Indagación técnica
  - o Confirmación tecnológica
  - o Cálculo Matemático
  - o Análisis de tendencia
- ❖ Comprobación

La estructura procedimental, se halla regulada por la normativa señalada en la figura 28, ratificando en el entorno computacional su equivalente en la criminalística forense, la cataloga como: a)Objeto, b)Instrumento, c)Huella, d)Marca y e)Rastro y Señal; Para con base a esto fundamentar el proceso investigativo y determina:

- ❖ Identificación de Autores
- ❖ Pruebas de ejecución del hecho
- ❖ Reconstrucción de la operación

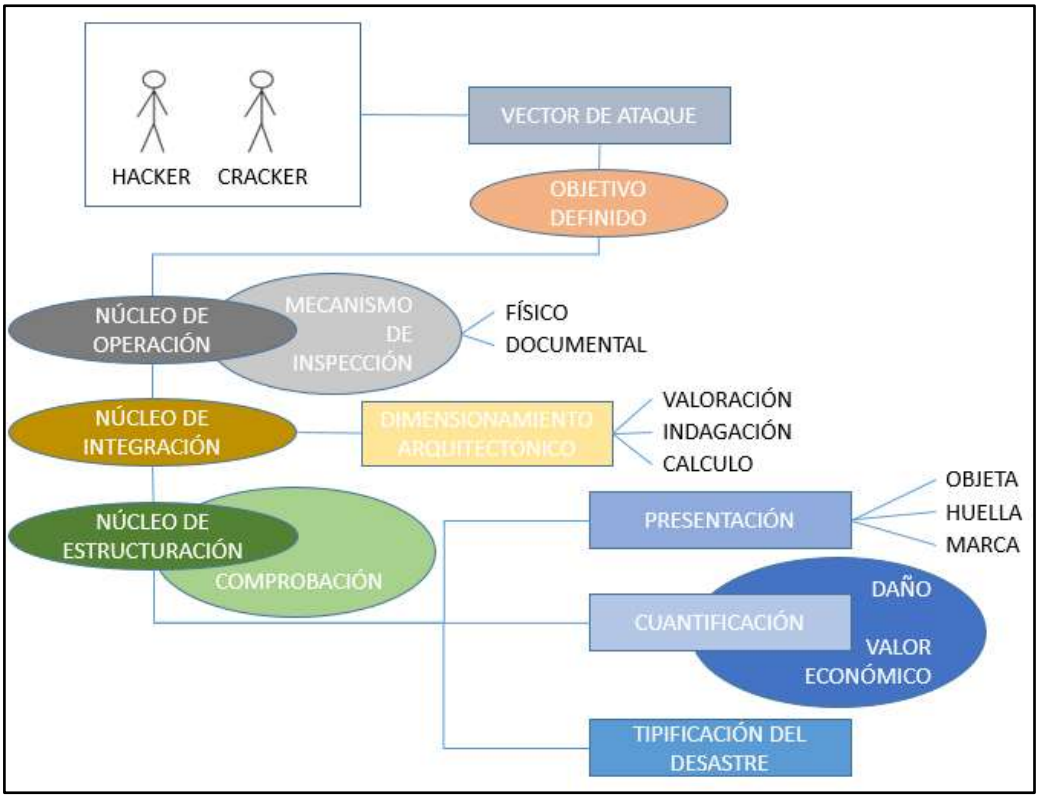


Figura 28: Estructura Procedimental De La Evidencia

Fuente: Aporte realizadores

Generalmente la técnica procedimental en el espacio geométrico computacional, se define al considerar la base jurídica construida experimentalmente [Mirkovic 2005]

- Dogmática Jurídica: Concepto de Delito informático
- Clasificación Jurídico Penal: a)Instrumento, b)Fin
- Conducta Tipificante: a)Acción, b)Omisión, c)Tipicidad y d)Atipicidad
- Antijuricidad: a)Imputabilidad, b)Inimputabilidad
- Culpabilidad y Ausencia: a)Formas de Culpabilidad, b)Ausencia de Culpabilidad
- Punibilidad y ausencia: a)Excusa absolutoria, b)Tentativa, c)Consumación, d)Conducta delictiva, e)Conducta nociva, f)Mundo virtual y g)Terrorismo cibernético

- Política en la criminalística informática

En la figura 29, se referencia a nivel de ejemplo el proceso de observación para estructurar una evidencia de ataque a un disco duro, para la cual considera la tipología de falencias que se enuncian: a) Lógica, b) Electrónica, c) Mecánica y d) Firmware

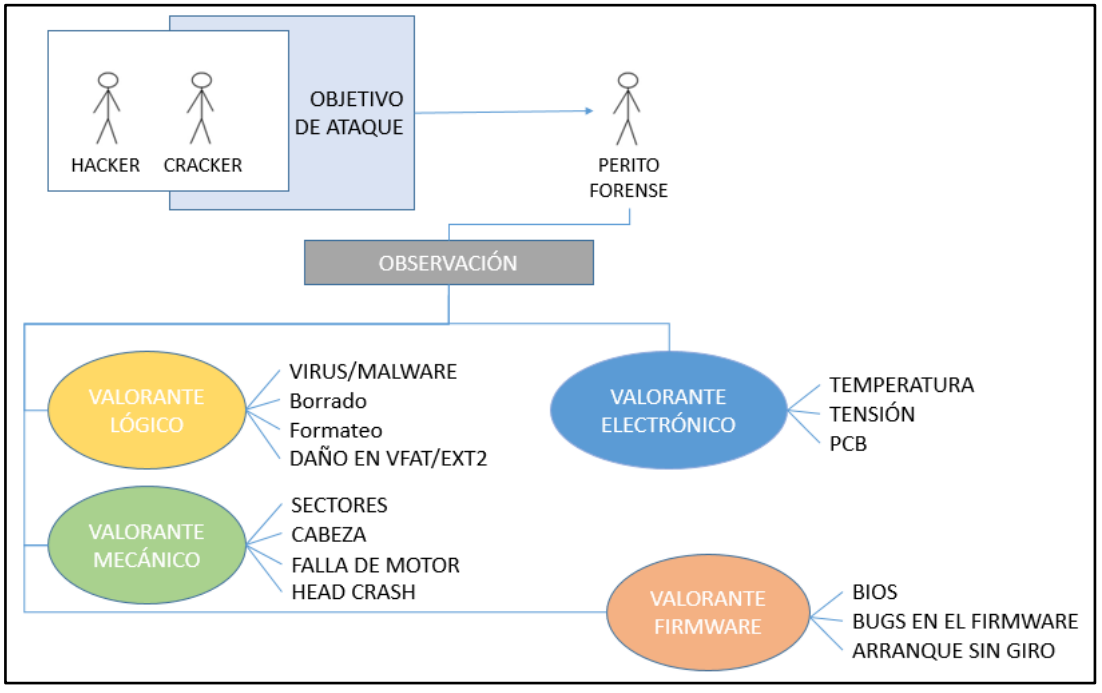


Figura 29: Casuística Sistémica Observación Disco

Fuente: Aporte Realizadores

3.3. PROCESO DE ESTRUCTURACION

La estructuración de la evidencia producto del impacto del ataque registrado, depende sistémica e integralmente del proceso de observación, de la analítica operacional aplicada y de la relación disciplinar de las fuentes integradoras que soportan o determinan la secuencia logística de los implicantes localizados en el espacio de registro del incidente informático, con el fin de ratificar la presencia de la trilogía señalada: Observación – Analítica – Relación Disciplinar, se presentan como base sustantiva para estructurar el modelo que se tratara con profundidad en el siguiente numeral, los casos de referenciación que a nivel de ejemplo, se señalan a continuación:

3.3.1. CASO 1: CONSIDERACIÓN PROBABILISTICA

El experto en informática forense, puede estructura el proceso de acopio o análisis de indicios o evidencias, valorando el registro estadístico asociado con los esquemas de atención y ocurrencia que con su observación o indagación registre, para la cual deberá considerar:

- **Unión de probabilidades:** $P(E_1\,UE_2) = P(E_1) + P(E_2) - P(E_1ME_{2)}$ (10)
- **Probabilidad de ocurrencias de fallas:** $P(F) = \sum_{i=1}^{n} P(Ei)\,.P(F|Ei)$ (11)
- **Interseccion de la probabilidad**: $P(E_1 \cap E_2) = P(E_1).P(E_2)$ (12)
- **Teorema de Bayes**: $P(Ei|F) = \frac{P(Ei).P(F|Ei)}{\sum_{i=0}^{n} P\,(Ei).P(\overline{F}|\overline{Ei})}$ (13)

Cuyo manejo se ilustra con estos objetos de estudio, a saber [Rheault 2002]

3.3.1.1. OBJETO DE REFERENCIA

Una red está definida por tres servidores SA=Servidor de Correo, SB=Servidor de Base de Datos y SC=Servidor de Comunicaciones, cuya frecuencia operacional de trabajo es respectivamente 255, 45% Y 30%, El registro de frecuencia de ataque asociado con cada servidor es de 0.10, 0.25, 0.18. Cuál es la probabilidad de que la red se congele o falle por evidenciar un ataque en cualquier servidor

P(SA) = 0.25 P(F|SA) = 0.10

P(SB) = 0.45 P(F|SB) = 0.25

P(SC) = 0.30 P(F|SC) = 0.18

Mediante la formulación de la regla de eliminación, el experto forense estima la probabilidad de falla o congelación por ataque a un servidor

$$P(F) = \sum_{i=0}^{n} P(Ei).P(F|Ei)$$

$$P(F) = \sum_{i=0}^{3} P(Ei).P(F|Ei)$$

$$P(F) = P(SA).P(F|SA) + P(SB).P(F|SB) + P(SC).P(F|SC)$$

$$P(F) = (0.25).(0.10) + (0.45).(0.25) + (0.30).(0.18)$$

$$P(F) = (0.025) + (0.1125) + (0.054)$$

$$P(F) = 0.1915 = 0.20 = 20\%$$

Cuyo valor bajo, le permitirá al perito investigador, concluir que la falla provocada en el sistema no es posible que prevenga del ataque de intrusos.

3.3.1.2. OBJETO DE REFERENCIA 2

El experto forense, quiere valorar en la misma situación la probabilidad de congelación de sistema telemático, operando esta información.

- Frecuencia operacional por servidor

  P(SA) = 0.40

  P(SB) = 0.28

  P(SC) = 0.32

- Frecuencia o evidencia de falla por servidor

  P(F|SA) = 0.06

  P(F|SB) = 0.10

  P(F|SC) = 0.12

Si se quiere proyectar o determinar la probabilidad de caída de la red, al registrarse un ataque al servidor SA, el experto deberá utilizar el teorema de Bayes

$$P(Ei|F) = \frac{P(Ei).P(F|Ei)}{\sum_{i=0}^{n} P\ (Ei).P(F|Ei)}$$

$$P(Ei|F) = \frac{(0.40).(0.06)}{(0.40).(0.06) + (0.28).(0.10) + (0.32).(0.12)}$$

$$P(Ei|F) = \frac{0.024}{0.024 + 0.028 + 0.038}$$

$$P(Ei|F) = \frac{0.024}{0.0904}$$

$$P(Ei|F) = 0.265 = 0.27 = 27\%$$

El manejo de la teoría de probabilidades, le permite al experto consolidar su visión de certidumbre al pretender estructurar la evidencia que se busca

3.3.2. CASO 2: ANALISIS SEMANTICA RPC

El dialogo cliente-servidor, al emplear conectividad de alto nivel como RPC (Remote Procedure Call), puede habilitar problemas de congelación o caída del sistema, cuya observación objetiva determinara la construcción de la evidencia [Tanenbaum 2012], considerándose la casuística siguiente.

- El cliente se cae luego de enviar una transmisión
- El cliente espera respuesta del servido, pero no puede recibirla
- El servidor falla cuando recibe una transacción y empieza a procesarla
- La transacción enviada por el cliente nunca llega al servidor
- El cliente no ubica el servidor

El análisis correspondiente de estos escenarios de estudio, exige que el experto en informática forense recurra al análisis de los factores mostrados en la figura 30.

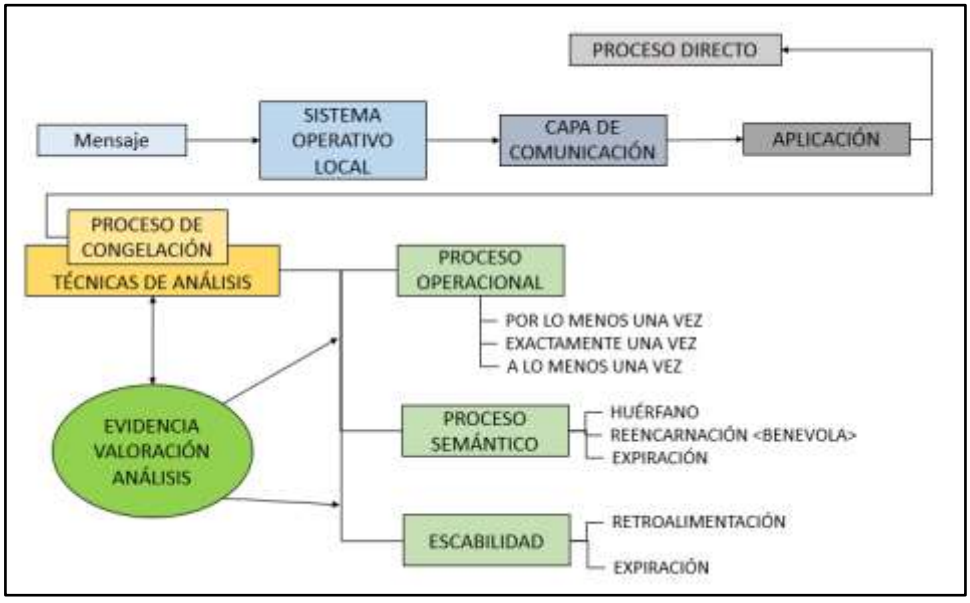


Figura 30: Casuística De Fallas RPC

Fuente: Aporte Realizadores

Debiéndose también considerar lo pertinente a las condiciones relacionadas con:

- Multitransmisión Atómica[38]

[38]Procedimiento de enlace distribuido que permite la emisión o recepción de valores informáticos sobre arquitecturas heterogéneas para consolidar el eje de trasmisión.
http://www.academia.edu/21420808/sistemas_distribuidos_sistemas_distribuidos_principios_y_paradigmas

- Sincronía Virtual[39]
- Multitransmisión causal
- Multitransmisión Fifo
- Realización Bifásica (2PC:two Phase Commit Protocolo)
- Realización Trifásica (3PC:Three Phase Commit Protocolo)
- Proceso de Recuperación
- Protocolo de Registro Pesimista
- Protocolo de Registro Optimista

El análisis relacionado, enmarca la construcción de evidencias por el control de recuperación [Elnozahy 2004], hecho que exige por ende la relación interpretativa de los aspectos definidos por la arquitectura de seguridad GLOBUS [Chevenak 2005], que cataloga como pilares de operación los factores listados aquí:

- El ambiente operacional direcciona múltiples dominios
- Las operaciones locales dependen de políticas de seguridad definidas por el dominio local
- Las operaciones globales son aceptadas por cada dominio
- La autentificación global reemplaza a la realizada por un dominio local
- El acceso a los recursos se define por la normativa de seguridad de cada dominio local
- Los procesos pueden heredar derechos delegado por usuarios
- Los procesos en un dominio local puede compartir credenciales

Con este ejemplo o caso de referenciación, se confirma que la estructuración de evidencias no es el resultado de solo interrogar o mirar un espacio, se hace imprescindible utilizar una sólida fundamentación de las ciencias de computación y la seguridad informática, razón por la cual es condición necesaria y suficiente en informática forense que se ocupa de la construcción de evidencias, acredite el dominio temático de las disciplinas mostradas por la figura 31 [Cano 2015].

[39]Procedimiento de concurrencia y cooperación que permite replicar transaccionalmente unidades de información sobre un espacio de múltiple cubrimiento por validación del Middleware.
http://www.academia.edu/21420808/sistemas_distribuidos_sistemas_distribuidos_principios_y_paradigmas

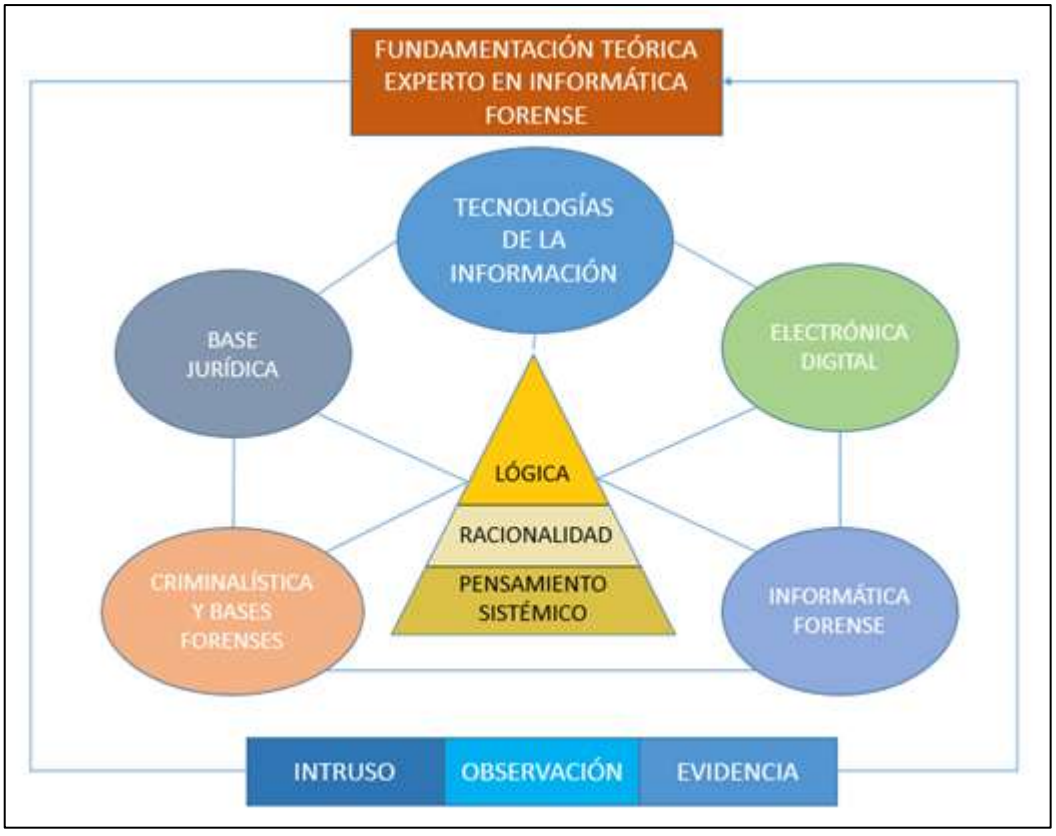


Figura 31: Espectro del Dominio Teórico del Experto

Fuente: Aporte realizadores

La prueba que se estructure en el proceso investigativo forense en el campo de la informática, debe validar con holgura, la llamada función de verosimilitud [Obregón 2015], que determinara la probabilidad de observar lo que realmente se observó, cuyo estimador se define asociado con la distribución normal cuyo tratamiento matemático conlleva a considerar como referentes las ecuaciones que se listan en el universo de la teoría de probabilidades.

$$fx(X,\alpha,\sigma) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2\sigma^2}(Xi-\alpha)^2} \quad (14)$$

$$L(\alpha,\sigma,X) = \prod_{i=1}^{\mu} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2\sigma^2}(X_2-\alpha)^2} \quad (15)$$

$$L(\alpha,\sigma,X) = \frac{1}{\sigma^{n(2\pi)^{n/2}}} e^{\frac{1}{2\sigma^2}(Xi-\alpha)^2} \quad (16)$$

$$L(\alpha,\sigma) = \log L\,(\alpha,\sigma) \quad (17)$$

$$= -M\log\sigma - \frac{1}{2\sigma^2}\sum_{i=1}^{n}(Xi-\alpha)^2 \quad (18)$$

$$\frac{\partial L}{\partial \sigma} = -\frac{n}{\sigma} + \frac{1}{\sigma^3} \sum (Xi - \alpha)^2 = 0 \text{ (19)}$$

$$\frac{\partial L}{\partial \alpha} = -\frac{1}{2\sigma^2} \sum_{i=0}^{n} 2(X_2 - \alpha) = 0 \text{ (20)}$$

Que determina

$$\alpha = \frac{\sum_{i=1}^{n} Xi}{n} \text{ (21)}$$

$$\sigma^2 = \frac{1}{n} \sum (X_2 - \frac{\sum X_2}{n})^2 \text{ (22)}$$

Las herramientas de mayor reconocimiento en el contexto de la informática forense son:

- Herramientas Hardware: en el segmento capitular anterior se listaron algunos ejemplos representativos
- Herramientas de Software
  - Análisis de Memoria
    - PD
    - FTK Imager
    - Dumplit
    - Volatility
    - Memorize
  - Montaje y Acceso de Discos
    - Imdisk
    - OSFmount
    - FTK Imager
    - Liveview
    - Mount Image Pro
    - Scalpel
    - Recovers
    - IEF
    - MFT Parser
    - Prefetch Parser
  - Análisis de Malware
    - Pdf Tools
    - Capture Bat

- Firebug
- Rzadare
- Shellcode 2 exe

- Manejo de Red
  - Wireshark
  - Xplico
  - Snort
  - SplunkIphone
  - Alienvault
- Recuperacion de Pasaportes
  - NTPWedit
  - NTPasswd
  - PWdump7
  - Saminside
  - OPcrash
  - Lophtcrack
- Dispositivos móviles
  - Iphone Browser
  - Iphone Data Protection
  - Blackberry Desktop
  - Phoneminer
  - Osaf

3.3.3. CASO 3: VALORACION POLÍTICAS DE SEGURIDAD

Frente a un incidente o delito informático cometido, el experto en informática forense deberá examinar los servicios y mecanismos de protección según especificaciones X.800, nativas de protección de redes ópticas, básicas de expansión a nivel de lenguaje o mediante evaluación del parámetro de operación de la tecnología sólida.

3.3.3.1. ESPECIFICACIONES OPERACIONALES X.800

El enfoque sistemático asociado con la arquitectura de seguridad OSI que detecta o previene los ataques o mejora la seguridad definida, cataloga esta plataforma. [Stallings 2012]

- Servicios
  - Autentificación: a)De Entidades, b)De Datos
  - Control de Acceso
  - Confidencialidad: a)De conexión, b)De orientación, c)Flujo de tráfico y d)De campos seleccionados
  - Integridad de Datos: a)De conexión con recuperación, b)De conexión sin recuperación, c)De conexión con campos seleccionados y d)No orientado a conexión
  - No Repudio: a)De origen, b)De destino
- Mecanismos de Operación: a)Cifrado, b)Firma digital, c)Integridad de Datos, d)Intercambio de Autentificación, e)Relleno de Trafico, f)Control de Enrutamiento y g)Notarización
- Mecanismos de valoración global: a)Funcionabilidad fiable, b)Etiquetas de seguridad, c)De acciones, d)De auditoria y e)De recuperación

3.3.3.2. PROTECCION DE OPERACIÓN DE ENLACE

Todo experto en informática forense, que enfrenta el proceso de acopio de evidencias dentro de un sistema telemático, debe estar familiarizado con la normativa ITU-T M.3400, que cataloga las funciones de gestión en la red a saber: a)Frente a fallas, b)De configuración, c)De auditoria y contabilidad, d)De prestaciones y e)De seguridad [Capmany 2012]

Quiere esto decir, que el perito forense es conocedor por ejemplo al evaluar escenarios de comunicación óptica de los servicios de gestión de la capa óptica, de la gestión de alarmas, equipos y adaptación y por supuesto de la traza óptica como identificador de control para poder dimensionar estos indicadores. [Capmany 2000]

- ❖ OCPT (Optical Channel Path Trace) Actúa como aislante al detectar conexiones incorrectas
- ❖ OCST (Optical Channel Section Trace) Localiza conexiones y verifica integridad
- ❖ OCTST (Optical Channel-transparent section Trace) Indicador de control en los extremos

Convencionalmente, el experto está familiarizado con las fuentes de error más presentadas en los sistemas de interconexión, identificando:

- ❖ Errores Humanos
- ❖ Corte de Cable
- ❖ Retiro Equipo de Conexiones
- ❖ Operación Equivocada de Conmutadores
- ❖ Redundancia de Controladores y Fallas en Nodos
- ❖ Problemas de Conmutación
  - o Path Switching o de camino
  - o Span Switching o de enlace
  - o Ring Switching o de anillo
- ❖ Fallas en los esquemas de protección [Ramaswani 2002]
  - o OMS 1+1
  - o OMS 1:1
  - o OMS-DPRING
  - o OMS-SPRING
  - o OCH 1+1
  - o OCH-SPRING
  - o OCH-NESH

Finalmente para el análisis y evaluación situacional de inconvenientes o problemas de interconexión, se premisa estipular que todo experto en informática forense habrá de laborar con objetividad la estructura del estándar ASON[40] (Automatically Switched Optical Network): a)G.8080, b)G.7713, c)G.7714, d)G.7715; además de diferenciar la configuración y operación de las redes de

[40]Arquitectura operacional óptica que cataloga e integra la flexibilidad como unidad de distribución y configuración operacional de valores informáticos en una solución óptica.
http://transparencia.munilaunion.cl/Documentos/Tramites/_ocs.pdf

acceso, a saber, a)XDSL, b)ADSL, c)VDSL, d)FTTX: FTTH(Fiber To The Home) FTTB(Fiber To The Home Building) FTTC(Fiber To The Curb) FTTCAB(Fiber To The Cabinet) FTTEX(Fiber to the Exchange) [Varsalone 2009]

3.3.3.3. PATRONATO DE EXPANSION A NIVEL DE LENGUAJE

La ejecución de soluciones, requiere de la habilitación de permisos y de la integración de firma, por ejemplo con el lenguaje java, se hace fácil realizar estas operaciones [Froute 2012].

- Creación de archivos de políticas

```
Grant{
    Permission java.util.propertypermission “user.home”, “read”;
    Permission java.io.filepermission “{user.home}/textor.txt”, “write”;
    Permission java.io.filepermission “{user.home}/textol.txt”, “read”;
    };
```

- Ejecución con archivo de política.
- Reconstrucción de acceso a aplicaciones

```
Grant{
    Permission java.awt.awtpermission “accesseventqueue”;
    Permission java.awt.awtpermission “showwindowthoutwarningbanner”;
    Permission java.util.propertypermission “user.home”, “read”;
    Permission java.io.filepermission “{user.home}/textor.txt”, “write”;
    Permission java.io.filepermission “{user.home}/textol.txt”, “read”;
    };
```

- Firmado de Applets

  Con esta base teórica, el experto puede entonces identificar falencias operacionales producto del manejo, direccionamiento y encadenamiento de Applets intrusos que generaran perturbaciones en el sistema.

3.3.3.4. OPERACIÓN DE LA TECNOLOGIA DEL ESTADO SOLIDO

Todo experto en informática forense, dada su base de conocimientos para lograr la estructuración de solidas evidencias, debe siempre tener presente que su proceso está orientado a: a)Perseguir y permitir el proceso judicial de los intrusos o criminales informáticos, b)Valorar la compensación de los daños causados por los intrusos y c)Prevenir casos similares al formular estrategias solidas de seguridad

Por ello, el experto no debe estar ajeno al nuevo escenario de acción que cubre la tecnología del estado sólido, cuyo espectro de operación se resume en las llamadas unidades SSD y en las memorias FLASH caracterizada por [Cano 2015]:

- Soporte digital NAND/NOR
- Cohesión por oscilación
- Segmentación de almacenamiento y cache acelerada
- Atributo funcional independiente
  - NOR con lectura superior a NAND
  - NAND escribe con mayor velocidad
  - Borrado previo para efectuar operaciones de escritura
- Controlador FTL[41] (Flash Translation Layer) para traducción de memoria flash
- Menor consume de energía
- Eliminación total del ruido
- Segmentación por comando TRIM[42]

Con el desarrollo de la tecnología del estado sólido, el Iphone se convierte en objeto de ataque, por lo cual el experto en informática forense debe en primera instancia el cotejar con objetividad estos factores.

[41]Nivel de referenciación operacional para el control de almacenamiento y borrado de la memoria FLASH configurada sobre un dispositivo móvil http://www.stlinux.com/howto/Flash/FTL

[42]Comando que sobre un Iphone direcciona el espacio de almacenamiento para catalogación de archivos o valores informáticos con el fin de optimizar el direccionamiento lógico. http://windowsitpro.com/systems-management/q-what-trim-function-solid-state-disks-ssds-and-why-it-important

- Código de acceso Pin[43] y Puk[44]
- Código ICCID
- Código o factor IMEI[45]
- Dirección MAC Wifi
- Dirección MAC Bluetooth

El acceso explorativo sobre equipos móviles, lo realiza el perito forense contando con un equipo como el UFED que ofrece:

- Total compatibilidad
- Completa extracción de datos: a)Mensajes SAS, b)Imágenes, c)Videos, d)ENS/IMEI y e)Historial de borrado
- Copia de la ID: SIM

Esta solución se ha optimizado con la versión UFED 4PC que ofrece estas ventajas

- Las capacidades de la versión Ultimate de la solución incluyen:
  - Extracción física y decodificación a la vez que omite el bloqueo por patrón, pin o contraseña de dispositivos Android, incluyendo la familia Samsung Galaxy S, LG, HTC, Motorola y muchos más.
  - Extracción física y de sistema de archivos y decodificación de dispositivos Android ejecutando OS 4.2 – 4.4.3
  - Extracción física de dispositivos BlackBerry® ejecutando OS 4 – 7. Decodificación exclusiva: Datos BBM, apps, correos electrónicos, Bluetooth y otros.
  - Amplia compatibilidad con la extracción y decodificación de dispositivos Apple
  - Extracción física y decodificación de dispositivos Nokia BB5 bloqueados: extracción de contraseñas de dispositivos específicos
  - Acceso sin paralelo a dispositivos bloqueados omitiendo, revelando o deshabilitando el código de bloqueo del usuario

[43] Código de activación y direccionamiento operacional del Iphone https://support.apple.com/es-es/HT201529

[44] Unidad de control, rastreo y seguimiento del PIN para efectos de bloqueo o desbloqueo https://es.support.t-mobile.com/docs/DOC-31060

[45]Código de identificación y señalización a nivel direccional y de conectividad de un dispositivo móvil. https://support.apple.com/es-es/HT204073

- Extracción física y decodificación de dispositivos Windows Phone ejecutando OS 8.0 – 8.1
- Extracción de sistema de archivos de todos los dispositivos ejecutando Windows Phone, HTC, Samsung, Huawei y ZTE
- Recuperación de una mayor cantidad de datos eliminados del espacio sin asignar de la memoria flash del dispositivo
- Decodificación de extracciones físicas JTAG de un conjunto de datos enriquecidos
- Descifrado de registros de viaje TomTom® y extracción de datos de otros dispositivos GPS portátiles
- La base de datos cifrada del historial de WhatsApp que ahora se puede descifrar
- Conjunto de decodificación enriquecido: Datos de apps, contraseñas, correos electrónicos, historial de llamadas, SMS, contactos, agenda, archivos de medios, información de ubicación, etc.
- Capacidades exhaustivas de análisis a través de UFED Physical Analyzer, incluyendo línea de tiempo, analíticos de proyectos, detección de malware y listas de vigilancia
- Generador de reportes fáciles de leer, en una diversidad de formatos usando UFED Physical Analyzer
- Traducción de contenido en idioma extranjero desde sus extracciones, usando la solución de traducción fuera de línea de UFED Physical Analyzer

❖ Las capacidades de la versión Logical de la solución incluyen:

- Extracción lógica de datos: Datos de apps, contraseñas, IM (mensajería instantánea), contactos, SMS y MMS, correos electrónicos, agenda, multimedia, registro de llamadas, detalles del teléfono (IMEI/ESN), ICCID e IMSI, información de ubicación SIM (TMIS, MCC, MNC, LAC)
- Clonación forense de la ID de la SIM para aislar el teléfono de la actividad de la red durante el análisis Actualizaciones frecuentes del software que aseguran la compatibilidad con nuevos teléfonos a medida que ingresan en el mercado

3.4. FORMULACION DEL MODELO

En el escenario de la cibernética y la investigación de operaciones, el modelo es una realidad, o es el objeto, concepto o conjunto de relaciones que se utilizan para representar y estudiar de forma simple y comprensible la realidad [Ackof 1998].

Definición que el trasladarla al ámbito de la informática forense, para el acopio y estructura de evidencias traduce mejor selección de componentes, mayor precisión y amplio nivel de interrelación funcional; por su esquematización simbólica el modelo que se presenta como entregable de este proyecto, integra la codificación descriptiva del espacio geométrico donde se estudia el impacto del delito y se especifica procedimentalmente las operaciones algorítmicas requeridos la estructura sistémica de este modelo, puede ser visualizada a la figura 32.

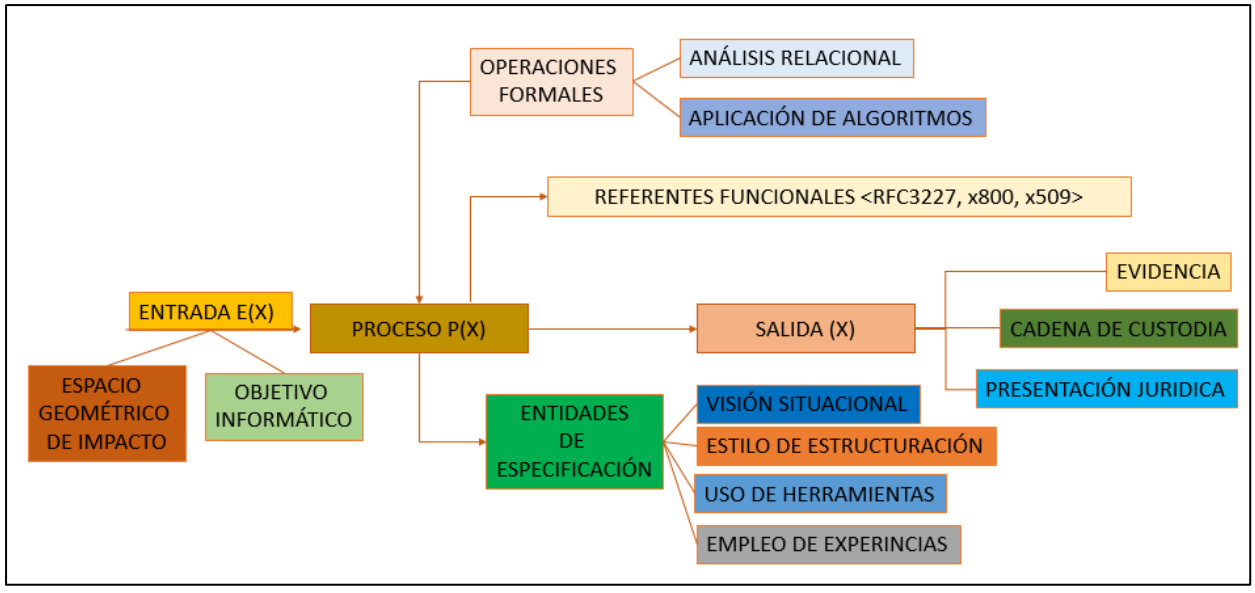


Figura 32: Estructura Sistémica del Modelo Propuesto

Fuente: Aporte Realizadores

3.4.1. ATRIBUTOS FUNCIONALES

El modelo desarrollado como producto de formación académica de la electiva informática forense en el programa de ingeniería de sistemas de la Universidad Libre de Colombia, refleja logísticamente estos atributos [Obregón 2002]

- Captura la imagen que constituye la esencia del espacio de impacto del ataque

- ❖ Valora y segmenta el espacio lógico o sistémico de análisis mediante la formulación de:
    - Función Objetiva: Medida de efectividad de la evidencia o indicio
    - Coeficientes Tecnológicos: base de estructuración computacional que se declaró como objetivo y herramientas forenses utilizadas
    - Marco de especificación Descriptiva: base de análisis formalizada por observación y estudio del espacio geométrico del ataque
- ❖ Base logística interpretativa
    - Hipótesis o suposiciones
    - Lenguaje de acción computacional para valoración del impacto generado
    - Funciones de manipulación del constructo base de indicio o evidencia

3.4.2. BASE SISTEMICA FUNCION P(X)

La función analítica procedimental, referenciada en la figura anterior, sustenta su significancia en la normativa RFC 3227 (https://www.rfc-editor.org/rfc/rfc3227.txt), cuya imagen de difusión se muestra en la figura 33 y cuyo contenido se registra en el anexo 3.

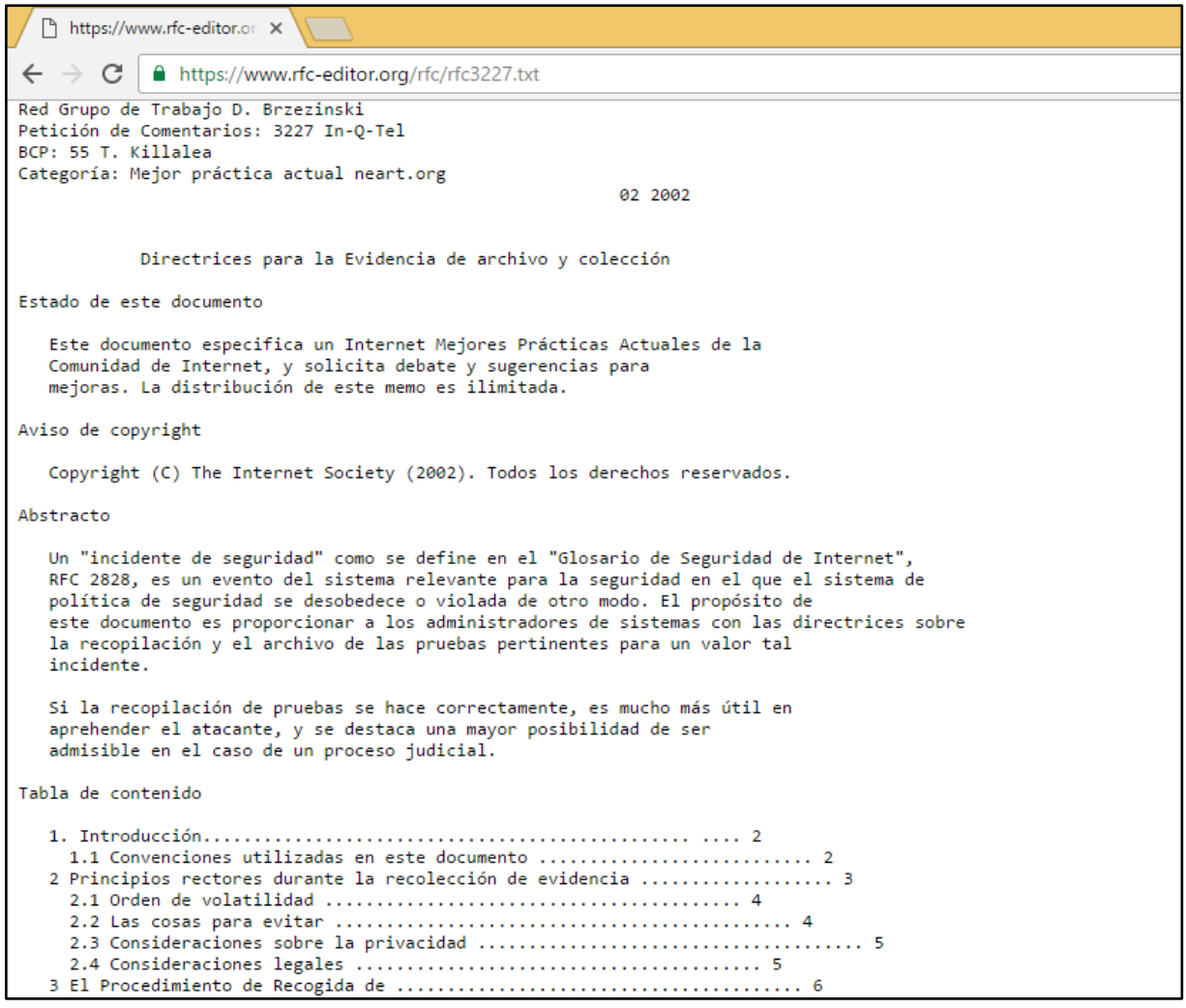


Figura 33: imagen de Difusión RFC3227

Fuente: https://www.rfc-editor.org/rfc/rfc3227.txt

Debiéndose también, para ampliar el dominio de definición de integridad que ha de poseer la evidencia que se estructura, el tener que sustentar la experiencia del investigador forense en el empleo de Rootkits o Exploit, que a nivel de ejemplo se despliegan en la dirección https://packetstormsecurity.com/ , cuya imagen se muestra en la figura 34.

Figura 34: Referente de difusión paquete de seguridad

Fuente: https://packetstormsecurity.com/

Con ayuda de la figura 35 se señalan los componentes operacionales de la función P(x), que define sistemáticamente al análisis forense digital, a saber [Lucas 2015]:

- Adquisición: copias Bit a Bit de la información impactada
  Imágenes fotocopias del espacio geográfico
- Preservación: técnica de Hashes para identificación de archivos y elaboración del acta para formalizar la cadena de custodia
- Análisis: evaluación ejes de impacto y consideración de la

criticidad del impacto generado

- Documentación: elaboración marco descriptivo de sucesos y detalles observados
- Presentación: informe técnico y ejecutivo base para el peritazgo judicial.

Las fases manifestadas de la función de proceso son: a) Identificación incidente, b) Recopilación Causal del incidente, c) Preservación evidencia, d) Análisis logístico de la evidencia jurídica del impacto.

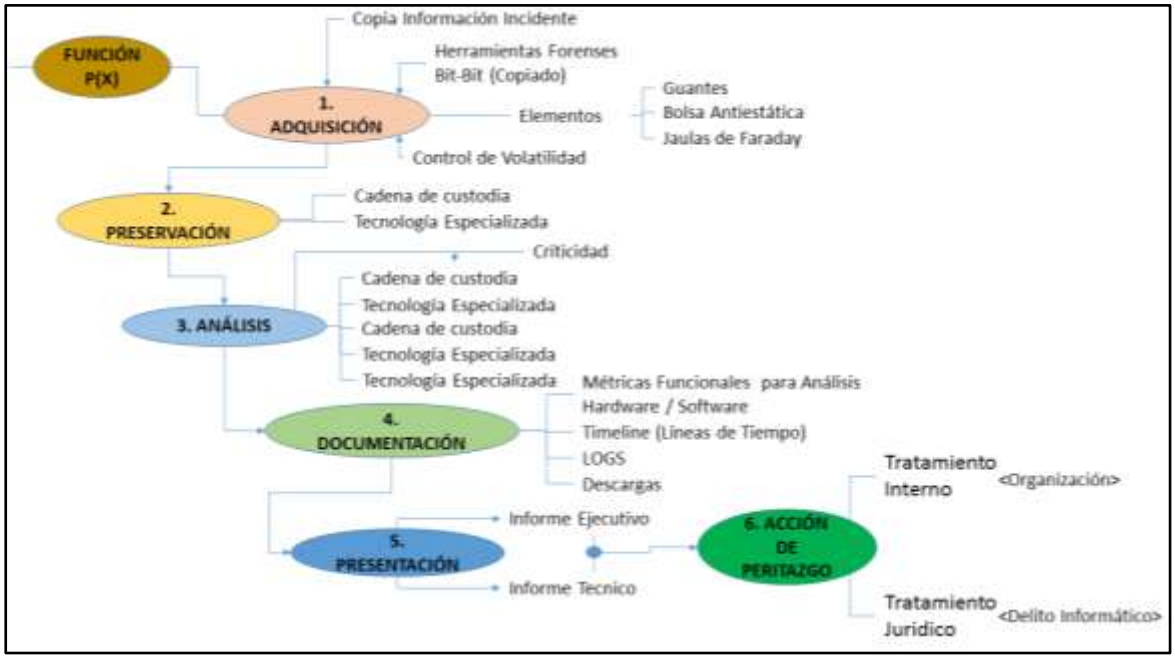


Figura 35: Componentes Función de Proceso P(X)

Fuente: aportes realizadores

3.4.3. ESPECIFICACION DE LA LOGISTICA DEL MODELO

El experto o investigador forense, responsable de la estructuración de la evidencia sobre el ataque producido, se ha de caracterizar por acreditar máxima racionalidad decisional [Rheault 2002], pues la construcción de la evidencia, presupone:

- Identificación conjunto de alternativas
- Poseer criterio decisional basado en el análisis sistémica de resultados, producto del empleo de la óptima base tecnológica
- Maximización de consecuencias
- Catalogación procedimental con algoritmos computacionales
- Validación de la trilogía causa – efecto – impacto o daño
- Facilidad interpretativa: Comunicación y comunicabilidad
- Minimización perdida de oportunidad: Diferencia entre resultado ideal y resultado obtenido
- Valoración descriptiva a nivel tecnológico del ¿que hubiese pasado?, del ¿Qué se pudo hacer? Y de ¿Cómo evitar la recepción?

Sistémica y situacionalmente el modelo definido con su función P(x), determina con sus operaciones formales para el análisis relacional la catalogación de dos entidades lógicas o escenarios de acción, a saber:

- Entidad 1: Discriminación de Incidentes
  - Código malicioso
  - Acceso no autorizado
  - Violación de políticas de uso o empleo
  - Denegación de servicio (DoS)
  - Catalogación de mecanismo propulsor de ataque
- Entidad 2: Base de Reacción
  - Gestión y actualización de espacio computacional
  - Configuración de servidores con privilegios mínimos
  - Definición de filtros perimetrales de tipo paranoico
    - IDS
    - ACL

- VPN
- Protocolos: IPSEC, SSL

- Plena y continua capacitación de usuario
- Base lógica procedimental de recuperación y restauración

3.4.4. LOGISTICA OPERACIONAL DEL MODELO

Los coeficientes tecnológicos y el marco de especificación descriptiva de permitirán formular la correspondiente función objetivo se estructurara a partir de:

- Interpretación del eje visual del impacto producido
- Catalogación de puertos TCP/UDP
- Conocimiento de directorio de usuarios
  - Nivel local
  - Enlace remoto
- Exploración zona horaria
- Identificación de procesos
- Mapeo direccional
  - IP
  - MAC
- Seguimiento mapeo destructivo
  - Archivos borrados
  - Archivos ocultos
  - Logs y registros del sistema
  - Examen soporte de seguridad
  - Generación funciones HASH
  - Copiado Bit a Bit
  - Análisis tráfico de red
- Formalización forense primigenio de evaluación[Cano 2015]
  - Registros y contenidos cache

- Vaciado de memoria
- Mapa funcional de red
  - Conexión
  - Ruteo
- Vaciado de Discos
- Vaciado unidades complementarias

- Calificación del impase o delito según normativa ley 1273
- Segmentación cadena de custodia

Los factor generador citados, son producto del estudio de la norma HB171 (Handbook Guidelines for the management of IT evidence) que regula la pertinencia a [Cano 2015]

- Diseño de evidencia
- Producción
- Recolección
- Análisis
- Reporte y presentación
- Determinación de relevancia de la evidencia

La logística que asocia el modo de operación del modelo sustenta los núcleos de acción procedimental que se listan [Cano 2015]:

- Validación de flujo generador
  - Registro de transacciones
  - Correo electrónico
  - Análisis de PC
  - Unidades de almacenamiento
- Examen del LOG a SAM del sistema
  - Acceso directo a Log
  - Exploración del registro
- Validación interacción WEB

- Flujo de interacción
- Control de antivirus
- Prevención de intrusos

❖ Catalogación Soporte de recuperación

- Sistema de Backup
- Estructura PBX
- Segmentación electrónica y lógica

❖ Preparación sustento judicial

- Integridad de evidencia
- Protección de privacidad e intimidad del indicio elaborado
- Integridad cadena de custodia
- Suposiciones de defensa de pertinencia y validez de la evidencia

Nota: esta fase, demanda la presencia de un abogado con experiencia en el análisis de incidentes informáticos.

4. CONCLUSIONES

- La integración procedimental de las características del ciberterrorismo y la criminalística digital en un modelo de referenciación para la estructuración de evidencias, al valorar el impacto del delito cometido, facilitara asociar la preponderancia de la prueba digital con su significancia, tal como lo especifica la estructura legal y normativa para el peritazgo.

- La consideración de la cadena de custodia como plataforma generadora de la veracidad de la prueba digital, permite identificar en el ecosistema afectado los indicios, los mecanismos y la trazabilidad humana, física y lógica, con las cuales se habrá de definir el protocolo requerido para cualificar el proceso pericial informático forense que valorará el juez de la república de Colombia

- La base de acción definida por el modelo formulado, que permite el acopio de evidencias, está orientada a permitir la recolección de elementos informáticos dubitados físicos o virtuales para lograr resguardar la prueba y determinar el traslado de la evidencia, permitiendo el proceder a secuestrar, decomisar, incautar o expropiar los objetos que el perito forense considere como fundamentales para la realización de la investigación que se adelanta.

5. RECOMENDACIONES

- Para validar el contenido expuesto como sustento operacional del modelo construido, se precisa su difusión al interior de la clase magistral de la asignatura Informática Forense.

- Con el fin de aplicar la visión formal experimental de la solución, se hace necesario estructurar conversatorios académicos con grupos de investigación de criminalística de la facultad de derecho.

- Se hace necesario verificar con la comunidad académica del programa, el conocimiento de la normatividad legal expuesta en la ley 1273 del 2009, para determinar el proceso definido para recolectar y estructurar evidencias, según considerandos del modelo trabajado.

6. REFERENCIAS BIBLIOGRAFICAS

Textos y Publicaciones

- Ackof R. and Sasieni M. (1998) Fundamentals of Operation Research. Editorial Wiley and Sons.
- Agualimpia C. y Hernandez R. (2013). Análisis Forense en Dispositivos Móviles. Tesis de Maestría Universidad Javeriana
- Bace R. and Mell R. (2000). Intrusion Detection Systems. Editorial Macmillan Technical Publishing
- Bishop M. (2006). Computer Security: Art And Science. Editorial Addison Wesley
- Brings A. and Jamieson R. (2003). Legal Issues For Computer Forensics. Proceedings For 14th Australians Conference On Informatic Systems. Perth Western Australia
- Cano M. Jenny. (2015). Computación Forense: Descubrimientos De Rastros Informáticos Segunda Edición. Editorial Alfaomega
- Capmany Francoy José y Ortega Tamarit Beatriz.(2007). Redes Ópticas. Editorial linusa
- Chervenak A., Foster L. and Kesselman C. (2005). The Data Grid: Towards And Architecture For The Distributed System. Editorial j. Netw. Computational
- Documento Consejo Nacional De Planeacion. (2010). Politicas De Ciberseguridad Y Ciberdefensa Minhacienda, MINTIC y Departamento Funcional De Planeación 3710
- Doorn J. and Rivero L. (2002). Database Integrity: Challanges and Solutions. Editorial Idea Group
- Elnozahy E. and Plack J. (2004). Checkpoint For Petascale Systems: A Look Into The Future IEEE Transactions Secure Computational. Number 34
- Froufe Quintas Agustín. (2009). Java 2: Manual de Usuario y Tutorial 5ta edición. Editorial Alfaomega
- Garcia Molina H. (2013). Elections In A Distributed System. IEEE Transaction Computer. Number 31
- Gollman D. (2006). Computer Security. Editorial John Wiley
- Kopetz H. and Verissimo P. (2003). Real Time And Dependability Concepts. Editorial Addison Wesley

- Lopez Calvo P. y Gomez Silva P. (2003). Investigación Criminal Y Criminalística Segunda Edición. Editorial Lenis
- Lua E. and Sharma R. (2005). On The Robustness Of Soft State Protocols. Procceding 12th International Conference on Network Protocols. IEEE Computer Security Press
- Lucas Paus. (2015). 5 Fases Fundamentales Del Análisis Forense Digital. Publicación Welivesecurity
- Martin Jose Maria. (2012). Hardware Microinformatico. Editorial Alfaomega
- Mchugh J., Christie A. and Alkent. (2000). The Role Of Intrusion Detection System. IEEE Transaction Software September-October
- Mirkovic J. and Reiher P. (2005). Internet Denial Of Service: Attack And Defense Mechanisms. Editorial Prentice Hall
- Nachenberg C. (2003). Computer Virus.Antivirus Coevolution Communications Of The ACM Magazine
- Obregón Sanin Iván. (1998). Teoría De La Probabilidad. Editorial Linusa
- Osterburg J. and Ward R. (2000). Criminal Investigation. Editorial Anderson Publishing
- Pfleeger C. (2006). Security In Computing. Editorial Prentice Hall
- Ramaswami R. and Sivarajan K. (2002). Optical Networks: A Practical Perspective. Editorial Morgan Kauffman Series In Networking
- Rheault Jean Paul. (2002). Introduccion A La Teoria De Las Decisiones. Editorial Linusa
- Riofrio J.C. (2204). La Prueba Electronica. Editorial Temis
- Stallings William. (2008). Fundamentos De Seguridad De Redes: Aplicaciones Y Estándares 2da Edición. Editorial Pearson
- Tanenbaum Andrew y Van Steen Maraton.(2012). Sistemas Distribuidos Principios Y Paradigmas. Editorial Pearson
- Varsalones and Kubasiak. (2009). Mac OS X, Ipod And Iphone Forensic Analysis Dud Toolkil. Editorial Syngress Publisshing Ing

Cibergrafia

- Iphone Comparation Tecnic. Apple incorporations (2014). http://www.apple.com/la/iphone Recuperado Septiembre 16/2016
- Cloud Computing: Another Digital Forensic Challenge (2009). http://www.forensicmagic.com/article/cloud_computing Recuperado Septiembre 18/2016
- Admisibilidad De La Audiencia Digital: De Los Conceptos Legales A La Práctica (2012). http://www.alfa_redi.org/rdi_articulo.shtm Recuperado Septiembre 30/A Hardware Based Memory Adquisition Procedure For Digital Investigation (2002). http://www.digital-evidence.org Recuperado Septiembre 30/2016
- Overview of attack trends (2002). http://www.cert.org/archive Recuperado Octubre 5/2016
- Hackers Beware. Defending Your Network From Wiley Hacker (2008) http://www.all.net Recuperado Octubre 7/2016
- Convention On Cibercrime (2010). http://www.conventions.coe.int/tremty/en/tremties Recuperado Octubre 12/2016
- Anatomy Of Linux Flash File Systems (2008). http://www.ibm.com/developerworks/linux Recuperado Octubre 12/2016
- Computer Forensics: The Need For Standardization And Certfication (2004) https://utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf Recuperado Octubre 14/2016
- Solid States Drives : Data Reliability And Lifeting (2008) http://csee.umbc.edu Recuperado Octubre 15/2016
- An Examination Of Digital Forensic Model (2012) http://www.utica.edu/academic Recuperado Octubre 17/2016
- Rock Solid: Will Digital Forensic Crack SSD? (2012) http://resources.infosecinstitute.com/ssd-forensics/ Recuperado octubre 23/2016
- Internet Trends: Presentation (2010) http://www.morganstanley.com Recuperado Octubre 25/2016
- Digital Forensic Research Workshop (2015) https://www.dfrws.org/ Recuperado Octubre 28/2016

- A Ten Step Process For Forensic Readiness (2004) https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf Recuperado Noviembre 5/2016
- Agenda De Ciberseguridad Global (2008) http://www.itu.int/cybersecurity recuperado el 12/2016
- Forensic Computing CSRC Research Project (2012) http://csrc.lse.ac.uk/people/sommerp Recuperado Noviembre 20/2016

ESPECIFICACION DESCRIPTIVA POR ANEXO

- **ANEXO 1:** Ley 1273
  - Objetivo: Presentar la normativa legal contemplada penalmente como acción para contrarrestar el delito informático en Colombia.
  - Fuente: http://www.mintic.gov.co/portal/604/w3-article-3705.html

- **ANEXO 2:** Sentencia sp1245-2015 del 11 de febrero del 2015
  - Objetivo: Mostrar como elemento de consideración y valoración frente al juez de la republica la integridad de una evidencia orientada a establecer si el delito de hurto por medios informáticos y semejantes admite la figura de la reparación integral, señalando la importancia del registro integral de cadena de custodia para lograr así la penalización correspondiente.
  - Fuente: http://www.cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1mar2015/SP1245-2015.pdf

- **ANEXO 3:** Normativa RFC 3227
  - Objetivo: presentar el desarrollo formulado por los ingenieros Dominique Brezinski y Tom Killalea, quienes al servicio de la firma NWG (Network Working Group), definieron las directrices que el experto en informática foresnse debe considerar para recopilar, analizar y evaluar los indicios y evidencias.
  - Fuente: http://wh0s.org/2014/06/20/estandares-de-manipulacion-de-pruebas-digitales-rfc-3227/

ANEXO 1: Ley 1273

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

EL CONGRESO DE COLOMBIA

DECRETA:

Artículo 1°. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor:

CAPITULO. I

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el

ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO. II

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Artículo 2°. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Artículo 58. Circunstancias de mayor punibilidad. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

(...)

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

Artículo 3°. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:

Artículo 37. De los Jueces Municipales. Los jueces penales municipales conocen:

(...)

6. De los delitos contenidos en el título VII Bis.

Artículo 4°. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal.

Hernán Andrade Serrano.

Presidente del honorable Senado de la República,

Emilio Ramón Otero Dajud.

El Secretario General del honorable Senado de la República,

Germán Varón Cotrino.

El Presidente de la honorable Cámara de Representantes,

Jesús Alfonso Rodríguez Camargo.

El Secretario General de la honorable Cámara de Representantes,

REPUBLICA DE COLOMBIA - GOBIERNO NACIONAL

Publíquese y cúmplase.

Dada en Bogotá, D. C., a 5 de enero de 2009.

ANEXO 2: Sentencia sp1245-2015 del 11 de febrero del 2015

CORTE SUPREMA DE JUSTICIA
SALA DE CASACIÓN PENAL

EYDER PATIÑO CABRERA
Magistrado ponente

SP1245-2015
Radicación n° 42.724

Bogotá D.C., once (11) de febrero de dos mil quince (2015).

MOTIVO DE LA DECISIÓN

La Corte decide el recurso de casación interpuesto por la defensora pública de CARLOS ARTURO ÁLVAREZ TRUJILLO contra la sentencia dictada el 29 de agosto de 2013 por la Sala Penal del Tribunal Superior de Neiva, que confirmó la proferida el 19 de julio del mismo año por el Juzgado Cuarto Penal del Circuito con funciones de conocimiento de esa ciudad, mediante la cual lo condenó en calidad de coautor del concurso de delitos de hurto por medios informáticos y semejantes agravado, concierto para delinquir y falsedad en documento privado.

HECHOS Y ACTUACIÓN PROCESAL RELEVANTE

1. Los primeros fueron sintetizados por el Tribunal de la siguiente manera:

(…) se estableció que existe una organización delictiva dedicada a clonar tarjetas de crédito y utilizarlas fraudulentamente con la participación de establecimientos comerciales y afectar a las entidades bancarias.

Se indicó que fueron identificados Pedro Vargas Perdomo, Dianne Carolina Barbosa López, Andrés Vargas Perdomo y Paola Andrea Rifaldo Ceballos, quienes se concertaron para obtener información de las bandas magnéticas de las tarjetas de crédito, las que registran en un computador y luego utilizan un magnetizador para grabarla en bandas y elaboran tarjetas falsas, contactan a los propietarios o administradores de establecimientos de comercio y les ofrecen el 40% o 50% como utilidades para la transacción ficticia, tal como ocurrió el 7 de diciembre de 2012 en el establecimiento comercial "Mucura" (sic) representado por Diego Mauricio Arias Ibáñez en el que se efectuó una compra ficticia por $7.000.000.00, y en el almacén Tennis & Tennis representado por Ricardo Jaime Sánchez Calderón se efectuó otra negociación ficticia por $8.000.000.00, contacto que fue realizado por Andrés Vargas Perdomo líder de la organización, quien inicialmente contactó a Carlos Arturo Álvarez Trujillo conocido como "Rata", el cual ubicó a Anibal (sic) Zamora Genneco para acercarse a los propietarios de los citados locales donde utilizaron la tarjeta clonada 4539387010020066 a nombre de Diana Paola Narváez que pertenece al banco Scotiabanc de Estados Unidos, en cuya banda magnética aparece el número (sic) 2666 8412 4521 7870 que corresponde al Chase Bank de ese país.

Se señaló que las tarjetas clonadas fueron enviadas desde Cali por la señora Dianne Carolina Barbosa López, siendo recibidas por la señora Esperanza Perdomo de Vargas quien se las entregó a su hijo Andrés Vargas Perdomo para ser utilizadas en los citados establecimientos comerciales, además, el último de los citados viajó en compañía de Carlos Arturo Álvarez Trujillo a Manizales a realizar más acciones delictivas sin que lo hubieran logrado porque las tarjetas no tenían cupo.

2. El 22 de diciembre de 2012, ante el Juzgado Tercero Penal Municipal con funciones de control de garantías de Neiva, se legalizaron las órdenes de interceptación de comunicaciones, el registro y allanamiento de algunos inmuebles, la incautación de elementos materiales probatorios respectiva y la captura de, entre otros, CARLOS ARTURO ÁLVAREZ TRUJILLO, oportunidad en la que el Fiscal Décimo Seccional de dicha ciudad le imputó los punibles de hurto por medios informáticos y semejantes, concierto para delinquir y falsedad en documento privado, previstos en los artículos 269I, 340 y 289 del Código Penal, en calidad de coautor, cargos a los que no se allanó. Igualmente, se le impuso medida de aseguramiento de detención preventiva en establecimiento carcelario.

3. Entre el imputado y la Fiscalía, el 14 de febrero de 2013 se celebró un preacuerdo en el que CARLOS ARTURO ÁLVAREZ TRUJILLO, asesorado por su defensora, aceptó su responsabilidad en los injustos endilgados, con la variación consistente en adicionar la circunstancia de menor punibilidad del artículo 55.1 y la de agravación específica, contemplada en el artículo 269H , respecto del delito de hurto por medios informáticos, a cambio de la imposición del mínimo de la sanción de este injusto, un incremento de 12 y 48 meses por los reatos concursantes –falsedad en documento privado y concierto para delinquir, en su orden- y una rebaja de pena del 45%, conforme al artículo 351 de la Ley 906 de 2004, para un monto definitivo de 92.4 meses de prisión. En el mismo documento se dejó constancia de que las víctimas fueron indemnizadas integralmente.

4. La verificación del preacuerdo se llevó a cabo por el Juez Cuarto Penal del Circuito con funciones de conocimiento de Neiva el 19 de julio siguiente, oportunidad en la que la Fiscalía precisó que el agravante imputado es el consagrado en el numeral primero del canon 269H y el representante de la víctima reiteró que fue indemnizado de manera integral.

5. Mediante sentencia de dicho día, el Juez de conocimiento condenó a CARLOS ARTURO ÁLVAREZ TRUJILLO, en calidad de coautor del injusto de hurto por medios informáticos y semejantes agravado, en concurso con los de concierto para delinquir y falsedad en documento privado, a la pena principal de noventa y dos (92) meses y doce (12) días de prisión y a la accesoria de inhabilitación para el ejercicio de derechos y funciones públicas, por igual término que la sanción privativa de la libertad.

Igualmente, se abstuvo de condenarlo en perjuicios y le negó la suspensión condicional de la ejecución de la pena y la prisión domiciliaria.

6. Recurrido el fallo por la defensa técnica de ÁLVAREZ TRUJILLO, el 29 de agosto de 2013 fue confirmado por una Sala de Decisión Penal del Tribunal Superior de Neiva.

7. La defensora pública interpuso y sustentó oportunamente el recurso extraordinario de casación, que fue admitido por la Corte el 8 de mayo de 2014.

8. La audiencia de sustentación oral correspondiente se llevó a cabo el 14 de noviembre siguiente.

LA DEMANDA

Tras identificar a las partes e intervinientes y la sentencia impugnada, transcribe la cuestión fáctica y procesal como fue sintetizada por el Tribunal, y al amparo de la causal primera del artículo 181 del Código de Procedimiento Penal invoca la violación directa de la ley sustancial por interpretación errónea del artículo 269I del Código Penal que conllevó a la falta de aplicación del canon 269 ejusdem.

Con el propósito de demostrarlo recuerda que para el ad quem no fue viable el reconocimiento de la rebaja punitiva, prevista en el aludido precepto 269, porque el delito de hurto por medios informáticos y semejantes no atenta contra el patrimonio económico.

Enseguida, transcribe, en extenso, algunos apartes del fallo acusado, en los cuales se asegura que, i) en este caso, el interés objeto de protección es la información y los datos ii) pese a que el punible en estudio puede ser pluriofensivo el mencionado descuento únicamente es posible respecto de los punibles señalados en el Título VII del Estatuto Sustantivo Penal, tal como lo ha reseñado la Sala de Casación Penal, iii) la Ley 1273 de 2009 creó un nuevo bien jurídico y unos delitos para garantizar la determinación informática, entre ellos, el de violación de datos personales, conducta que fue desplegada por el procesado.

A partir de dicha providencia, la defensora estima que el juez colegiado desatendió la clasificación e interpretación del tipo penal de hurto por medios informáticos y tergiversó una decisión de la Corte Suprema sobre un asunto en el que se pretendía obtener dicho beneficio respecto del delito autónomo de violación de datos personales.

Así mismo, destaca que el reato imputado tiene una estructura subordinada o complementaria, que requiere, para su comprensión, acudir al tipo básico o especial, esto es, al de hurto.

Agrega que el propósito del legislador fue salvaguardar el patrimonio y sancionar también el medio utilizado para la ejecución del ilícito.

En ese orden, es de la idea que «el SUPUESTO DE HECHO, se conforma con las dos disposiciones» , o sea, con las de los artículos 239 y 269I, razón por la cual considera válido afirmar que el legislador no únicamente sancionó la afectación del derecho a la intimidad sino también del patrimonio, máxime cuando «la redacción de la norma, da cuenta de que el fin principal o la acción reprochada es el apoderamiento de cosa mueble ajena, a más de recriminar el medio utilizado, es decir, el acceso a medios informáticos.»

Añade que si lo reprochado con el ilícito es el apoderamiento de cosa mueble, a través de medios informáticos, y la víctima es reparada, el procesado debe ser beneficiario del descuento consagrado en el canon 269, aspecto al que reduce la trascendencia del cargo postulado.

Cierra criticando al Tribunal por comparar el injusto de hurto por medios informáticos con el de apoderamiento de hidrocarburos, habida cuenta que este último está circunscrito a los delitos contra el orden económico y social, bien jurídico que, en criterio de la letrada «no es sujeto de indemnización, como si lo es el patrimonio de las personas» .

Solicita casar el fallo impugnado y proferir otro de reemplazo en el que se le conceda a su representado la rebaja de pena del canon 269 del Código Penal.

AUDIENCIA DE SUSTENTACIÓN ORAL

1.La defensa

Parte por reiterar que el único cargo propuesto tiene por propósito acreditar la infracción directa de la ley sustancial por interpretación errónea del artículo 269I del Código Penal, que condujo a la falta de aplicación del canon 269 ejusdem.

Tras destacar las razones que llevaron al Tribunal de Neiva a negar la rebaja punitiva por reparación integral a su prohijado, resalta que aquellas no solo desatienden la clasificación del tipo penal y su interpretación sino que tergiversan a la Corte cuando ella señaló que ese descuento era

improcedente entratándose del delito de violación de datos personales, habida cuenta su condición de delito autónomo que no afecta el patrimonio económico.

Destaca, asimismo, que el injusto de hurto por medios informáticos y semejantes es de naturaleza subordinada y requiere para su comprensión, acudir al tipo básico especial de hurto, consagrado en el artículo 239 del Código Penal.

En criterio de la jurista, es innegable que el precepto 269I remite a los delitos contra el patrimonio económico y que la intención del legislador fue resguardar este interés, sin importar el medio utilizado para birlarlo.

Para la comprensión del artículo 269I, dice, no se puede excluir el tipo básico de hurto, porque «el supuesto de hecho se conforma con las dos disposiciones que deben armonizarse» . Así, es de la idea que no solo se sanciona la lesión del derecho a la intimidad sino también el apoderamiento del patrimonio atacado por medios informáticos.

Añade que «el apoderamiento del patrimonio continúa con su entidad especial jurídica toda vez que la principal acción reprochada es el apoderamiento de una cosa o mueble ajena como lo dice el tipo base y es recriminar el medio utilizado, es decir, a título de agravante pero el tipo base necesariamente (…) deberá ser el del hurto inexorablemente (…)» .

Tras asegurar que la sentencia es el producto de un preacuerdo respecto de una imputación formulada contra 12 personas, advera que solamente a su representado no le fue concedido dicho beneficio y que el representante de la víctima está de acuerdo con su reconocimiento, debido a que fue indemnizada.

Para cerrar, solicita estimar lo dicho en la audiencia y lo consignado en el recurso de apelación, para que, con fundamento en la causal invocada, se case totalmente la sentencia impugnada y se emita fallo de reemplazo que conceda a su prohijado la rebaja punitiva prevista en el canon 269.

2. La Fiscalía.

El Fiscal Noveno Delegado ante la Sala de Casación Penal es del criterio que la pretensión de la demandante está llamada a prosperar.

Al respecto, inicia su disertación señalando que el problema jurídico se contrae a determinar si el hurto por medios informáticos y semejantes es un tipo penal autónomo o subordinado, a fin de establecer si es posible la aplicación de la diminuente consagrada en el artículo 269 de la Ley 599 de 2000.

Con tal propósito, alude a la clasificación de los tipos penales «atendiendo los vínculos que existan entre ellos, bien sea por los bienes jurídicos que salvaguardan o los elementos estructurales que les puedan ser comunes» , para, enseguida, diferenciar entre los de naturaleza autónoma y subordinada, destacando de los primeros que «gozan de estructura dogmática completa, por plena conjunción de los elementos que deben integrar el tipo penal, al punto que no es necesario que se asocien con otros para completar su ordenación típica» , mientras que los segundos «quedan siempre remitidos a un tipo principal, por razones de técnica legislativa, pues requieren de ellos para perfeccionarse por ausencia de alguno de los componentes necesarios para que tenga independencia normativa.»

Frente a los tipos subordinados, agrega, «deben interpretarse y adecuarse partiendo necesariamente del tipo básico del que dependen o se sirven, porque es éste el que contiene la descripción general como sujetos, conducta y objeto material, para después complementarla con los ingredientes propios de aquellos, que pueden ser normativos, subjetivos o referidos a la punición.»

En ese orden, contrario a lo estimado por el ad quem, cree que el artículo 269I no es un tipo autónomo sino incompleto y fragmentado, ya que incluso desde su nomen juris, remite, en cuanto al comportamiento reprobado, al tipo básico de hurto simple y, al hurto calificado, en punto de pena, de tal forma que únicamente enuncia «dos complementos descriptivos, referidos a la forma de ejecución o modo de comisión del delito, lo que descarta en él la condición de conducta típica básica o principal.»

Resalta que como el reato examinado no tiene verbo rector ni objeto material, estos elementos esenciales deben ubicarse en la acción de apoderamiento del hurto que recae sobre cosa mueble ajena.

A continuación, con apoyo en doctrina nacional, sostiene que el referido punible es de carácter pluriofensivo pese a su ubicación sistémica como delito informático, ya que no solo protege la información y los datos contenidos en sistemas electrónicos o virtuales, sino, de manera esencial, el patrimonio económico, porque «se trata intrínsecamente de la sustracción de bienes muebles ajenos, solo que a través de las tecnologías que allí se refieren como modalidades de ejecución del despojo patrimonial.»

A juicio del representante de la Fiscalía se incurrió en un error de técnica legislativa, pues las dos modalidades delictivas descritas en el canon 269I ejusdem «debieron hacerse concurrir como agravantes o calificantes del hurto, atendiendo su inconclusa descripción, al punto que el artículo 240 del C.P. ya contempla en su numeral 4° como circunstancia calificadora del hurto el que se cometa "violando o superando seguridades electrónicas y otras similares".»

Dicho lo anterior, concluye que la figura consagrada en el artículo 269 ibidem, puede ser aplicada «sistemática o extensivamente y no de manera gramatical o restrictiva» al hurto por medios informáticos, atendiendo los fines de la interpretación, concretamente, la búsqueda del sentido natural y obvio de la ley a través del contexto (artículo 30 del Código Civil) y su vocación práctica y correctiva.

En efecto, considera que de acuerdo con los modelos intermedios de positivismo normativista y de argumentación en los que se otorga primacía a los fines consecuencialistas y pragmáticos de la interpretación de los jueces, atemperados por los principios del derecho o normas rectoras, (constitucionalización) y los artículos 13 del Código Penal y 26 del Código de Procedimiento Penal, es viable sostener que «la decisión justa y prevalente frente al derecho sustancial es en este caso reconocer la aplicación de la diminuente por el resarcimiento del que habla el artículo 269 del Código Penal al punible de hurto por medios informáticos (…)» .

Añade que el precedente citado por el juez plural (auto del 13 de septiembre del 2013, radicado 37145) no es aplicable a este caso, debido a que el delito del que se ocupó es el de violación de datos personales, agravado, descrito en el artículo 269F sustantivo, que corresponde a un tipo penal

principal, completo y autónomo, ajeno a toda connotación patrimonial y la Corte no aseveró que a los delitos informáticos no se les puede aplicar la figura de reparación examinada sino que sólo cabe respecto de reatos contra el patrimonio económico.

Remata destacando que, en la audiencia de legalización del preacuerdo, el representante de la víctima expresó que el procesado restituyó el objeto material del delito e indemnizó los perjuicios ocasionados, por lo que se satisfacen los presupuestos exigidos por el artículo 269 sustantivo para que se disponga la disminución de la pena en los términos allí señalados.

En consecuencia, solicita casar la sentencia demandada y conceder la rebaja punitiva reclamada.

3. Representante de la Víctima

Se limita a reiterar que el acusado indemnizó integralmente a las entidades financieras por su participación en las conductas punibles imputadas, particularmente, en la clonación de tarjetas en los establecimientos comerciales y en la respectiva defraudación.

CONSIDERACIONES

1. El asunto que nos ocupa plantea varias cuestiones a dilucidar que, resueltas afirmativamente, lograrían dar respuesta al problema jurídico de mayor envergadura, consistente en establecer si el delito de hurto por medios informáticos y semejantes admite la figura de la reparación integral, descrita en el artículo 269 del Código Penal y, por ende, si los jueces de instancia incurrieron en la infracción directa de la ley sustancial por falta de aplicación de esa norma como consecuencia de la interpretación errónea del canon 269I ejusdem, al negar dicho derecho punitivo al procesado.

Para definir tal aspecto, la Corte adoptará como metodología de estudio la del conocimiento deductivo, para lo cual, como primer eje temático, examinará los elementos estructurales del aludido tipo penal y sus antecedentes legislativos para, con fundamento en ello, adentrarse en el análisis del bien jurídico protegido y la posibilidad de aplicar el criterio sistemático de interpretación y la analogía en bonam partem.

Finalmente, evaluará si el acusado puede o no ser beneficiario del descuento de pena por reparación integral de que trata el referido precepto 269, previsto para los injustos consagrados en el Título VII.

2. Antecedentes legislativos del delito de hurto por medios informáticos.

Debido a la creciente criminalidad en materia informática y a la necesidad de que Colombia alcanzara un nivel normativo similar al de otros países que, de tiempo atrás, venían sancionando infracciones relacionadas con el abuso de los sistemas informáticos y los datos personales –Convenio sobre la ciberdelincuencia de Budapest (2001), adoptado por el Consejo de Europa-, en el Congreso de la República surgió una primera iniciativa –Proyecto de Ley No. 042 de 2007 Cámara - destinada a modificar y adicionar algunos tipos penales regulados en el capítulo VII del Código Penal relativos a la «Violación a la intimidad, reserva e interceptación de comunicaciones» y a endurecer las penas del hurto calificado, el daño en bien ajeno, la violación de reserva industrial o comercial y el espionaje, cuando quiera que se ejecuten utilizando medios informáticos o se vulneren las seguridades informáticas de las víctimas.

La exposición de motivos fue expresa en señalar que, de los tres modelos legislativos posibles, a saber, i) ley especial –no integrada al Código Penal-, ii) capítulo especial –incorporado al Estatuto Sustantivo- y iii) modificación de los tipos penales existentes, se optó por el tercero a fin de garantizar la protección de otros bienes jurídicos distintos al de la información que también podían resultar lesionados con actividades relacionadas con la cibercriminalidad.

Así lo concibió el legislador:

Cuando se ha optado por una legislación o un capítulo especial que compendie los llamados delitos informáticos se ha partido de la base de la elevación a bien jurídico tutelado el derecho a la información, referida al dato informático (información almacenada, procesada y transmitida a través de sistemas informáticos), o si se quiere, el bien jurídico a salvaguardar es la seguridad informática, teniendo en cuenta que a través de su ataque se pueden vulnerar otros bienes como la intimidad, la

propiedad, la libre competencia y hasta la misma seguridad del Estado. Es por eso que algunos doctrinantes catalogan a ese derecho a la información o a la seguridad informática como bien jurídico intermedio que se hace digno de tutela penal, por su propio valor y por el peligro potencial que encierra su quebrantamiento para los demás bienes jurídicos.

Desde ese punto de vista han denominado al delito informático como una acción delictiva en la cual la computadora o los sistemas de procesamiento de datos han estado involucrados como material o como objeto de la misma; y se ha desarrollado el tema alrededor de la triple dimensión de los datos informáticos: confidencialidad, integridad y disponibilidad. Su respeto trae consigo un sentimiento de seguridad y tranquilidad a todos los asociados. De ahí que su transgresión deviene de la afectación de un derecho colectivo o supraindividual que por lo mismo debe ser digno de protección. Por eso es un bien intermedio para la afectación de derechos individuales.

(…)

Nuestra reciente tradición jurídica viene decantándose por la otra modalidad de legislación para este tipo de comportamientos consistente en la modificación de los tipos existentes para adecuarlos a la realidad, manteniendo tales conductas dentro de los capítulos correspondientes sin alterar los bienes jurídicos protegidos, y en esa dirección apunta el presente proyecto pues, como veremos, en gran parte de la iniciativa lo que se busca es agravar conductas actualmente tipificadas, o ampliarles el verbo rector, y solo en algunos casos se pretende tipificar comportamientos no contemplados en la ley penal.

La principal razón para optar por este camino es que son varias las conductas que si bien utilizan medios informáticos para la comisión de los delitos, bien puede asegurarse que no corresponderían a lo que se ha denominado delitos informáticos, sino que son delitos tradicionales remozados con nuevas formas de comisión, pero que ameritan un pronunciamiento expreso de la ley penal para aumentar su castigo dado la alarma social que genera la ruptura de la confianza que se deposita en una actividad cotidiana y necesaria de la vida moderna en la que el derecho a la información ha cobrado vida propia. (Subrayas no originales).

Posteriormente, surgió una segunda iniciativa legislativa –Proyecto de Ley No. 123 de 2007 Cámara -, con fundamento en un proyecto elaborado por un juez de la República y la asesoría de

algunos académicos patrios, la cual propuso la creación de un nuevo bien jurídico para la protección de la información.

Es así que, luego de la audiencia pública , en la que se enfatizó sobre la necesidad de proteger el patrimonio y los sistemas informáticos, se acumularon las dos propuestas legislativas en el Proyecto de Ley No. 042 Cámara, 123 Cámara y Senado , dando lugar a la proposición de crear un Título VII Bis al Código Penal, destinado, esencialmente, a la salvaguarda de la información y los datos, tomando como base, para el efecto, las conductas reguladas en el Convenio sobre la Ciberdelincuencia de Budapest y algunas que atentan contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, las cuales fueron ubicadas en el capítulo I y un segundo grupo de punibles definidos bajo el rótulo de "otras infracciones", concretamente, el hurto por medios informáticos y semejantes, la transferencia no consentida de activos, la falsedad informática, el espionaje informático, la violación de reserva industrial o comercial valiéndose de medios informáticos (capítulo II).

Separaron, pues, en dos conjuntos de normas, los atentados contra la confianza en el tráfico informático y los también lesivos de este bien y otros intereses jurídicos.

En esta oportunidad, explican los Informes de Ponencia para primer y segundo debate en Cámara que, se escogió el sistema legislativo consistente en confeccionar un título adicional para ser incluido en el texto del estatuto punitivo porque si bien, era más técnica la expedición de una ley especial, ella podría perderse «dentro de todo el entramado del ordenamiento jurídico, sin merecer la atención requerida por parte de estudiosos y administradores de Justicia, quienes, pretextando dificultades técnicas, falta de preparación, etc., prefieren dejar en el olvido este tipo de normatividades que terminan por no ser aplicadas o, si lo son, de una manera deficiente» y, asimismo, el modelo adoptado en el proyecto original -042- debido a que contraía «la dificultad de permitir la dispersión de esta problemática a lo largo del articulado lo que le quita fuerza y coherencia a la materia, (…) amén de que (sic) dificulta en extremo la precisión del bien jurídico que se debe proteger en estos casos, esto es, la Protección de la Información y de los Datos» .

Una afirmación como la recién transcrita podría sugerir un único valor jurídico a ser protegido: la información y los datos, pero son las mismas ponencias las que precisan frente a los punibles de hurto por medios informáticos y semejantes y transferencia no consentida de activos, que el primero procura «completar las descripciones típicas contenidas en los artículos 239 y siguientes del Código Penal, a las cuales se remite expresamente» y el segundo busca variar la estafa clásica por la figura de la estafa electrónica.

Repárese, en este punto, que, en relación con los otros delitos ubicados inicialmente en el capítulo II, los ponentes admitieron que además del interés por proteger la información y los datos también, pretendían salvaguardar bienes como la información privilegiada industrial, comercial, política o militar relacionada con la seguridad del Estado, en el caso del espionaje informático, y el orden económico y social, entratándose de la violación de reserva industrial o comercial.

El proyecto, así concebido fue aprobado en Cámara, pero en Senado su trámite sufrió algunas dificultades, al punto que la ponencia para primer debate en esa sede fue negativa y reclamó su archivo definitivo por considerarla innecesaria, de cara a la regulación penal existente para la fecha.

El ponente, luego de referirse a la tendencia colombiana a la hiperproducción de leyes y al casuismo; al derecho penal como ultima ratio y a la consecuente imposibilidad de dispensar una pronta y cumplida justicia; y a la importancia de acudir a los conceptos de «esencias y fenómenos» para distinguir entre el tipo penal con sus denominadores comunes o genéricos y sus modalidades, concluyó que no se deben «crear tipos con "nuevas" denominaciones o descripciones» pues «preexisten tipos que genéricamente recogen la esencia del comportamiento a reprimir» .

Particularmente, en cuanto se refiere al injusto de hurto por medios informáticos y semejantes, descrito en el artículo 269I, la ponencia señaló que se asimila al reato de hurto agravado y agregó que se observan los actuales artículos 239 y 240 de la (sic) C.P., dicha relación se establece sin ninguna modificación, pues el numeral cuarto del artículo 240 agrava el hurto con ganzúa, llave falsa superando seguridades electrónicas u otras semejantes. En consecuencia, no es correcto recalcar la relación ya existente.»

Sometido este informe a la aprobación de la Comisión Primera del Senado, se llegó al acuerdo de no archivar el proyecto, siempre que se hicieran algunos ajustes a los tipos penales, teniendo en cuenta, la creciente necesidad de regular las defraudaciones patrimoniales a los ahorradores de los sistemas financieros, «a quienes les copian por medios electrónicos –por ejemplo, las bandas magnéticas de las tarjetas de crédito a quienes les ingresan a las cuentas corrientes- y con claves descifradas transfieren fondos de una cuenta a otra y eso no es nuevo» .

El proyecto, con sus modificaciones –las que, en esencia, consistieron en eliminar del articulado los reatos de falsedad informática, espionaje informático y violación de reserva industrial o comercial - fue aprobado por la plenaria del Senado, por lo que se designó una Comisión de Conciliación que, finalmente, conservó como únicos delitos del capítulo II, los de hurto por medios informáticos y semejantes y transferencia no consentida de activos.

En este punto, es bueno precisar que ante las preocupaciones del senador GERMÁN NAVAS TALERO por la confusión que podría suscitarse en la definición del bien jurídico protegido en aquellos casos en que además de la información y los datos se atentara contra el patrimonio económico y la solución propuesta de agregar a los tipos básicos la modalidad informática y la inquietud del también senador OMAR DE JESÚS FLÓREZ VÉLEZ acerca del proyecto o la norma que se pretende aprobar, quedan debidamente protegidos, tutelados, los derechos de los ciudadanos, usuarios del sistema financiero, personas naturales y/o jurídicas, que sean objeto o víctimas de transacciones financieras, a través de la tecnología, a través de la utilización indebida, por parte de organizaciones criminales en la Internet» , uno de los ponentes –CARLOS ARTURO PIEDRAHITA CÁRDENAS- aclaró que aunque el bien jurídico protegido es el de la protección a la información y los datos, la nueva ley de la República procuraba amparar al sistema financiero y a sus usuarios de las defraudaciones patrimoniales.

El anterior recuento, permite establecer, objetivamente, que el nuevo título –VII bis-, se dirigió a regular, en esencia, el tema de los delitos informáticos y a proteger la información y los datos de carácter electrónico. No obstante, como quiera que uno de los actos más reprochados por la sociedad contemporánea involucra la utilización de los medios de procesamiento de datos para esquilmar los capitales de las personas naturales y jurídicas, además de regular comportamientos propiamente

característicos de la cibercriminalidad, el legislador colombiano utilizó esta oportunidad para enfatizar en la represión del apoderamiento ilícito, a través de mecanismos informáticos, de los dineros confiados al mercado financiero.

La Corte argumenta que el propósito del órgano legislativo fue acentuar, que no regular, por primera vez, el reproche jurídico-social respecto de dicha actividad ilegal porque ésta ya venía siendo sancionada conforme al punible de hurto, previsto en el artículo 239 del Código Penal, calificado por la circunstancia descrita en el numeral 4 del precepto 240 ibidem, tal como acertadamente destacaron varios de los congresistas en el debate parlamentario, con mayor énfasis, el senador PARMENIO CUÉLLAR en su informe de ponencia para primer debate en Senado.

En efecto, rezan dichas disposiciones:

ARTICULO 239. HURTO. <Penas aumentadas por el artículo 14 de la Ley 890 de 2004, a partir del 1o. de enero de 2005. El texto con las penas aumentadas es el siguiente:> El que se apodere de una cosa mueble ajena, con el propósito de obtener provecho para sí o para otro, incurrirá en prisión de treinta y dos (32) a ciento ocho (108) meses.

La pena será de prisión de dieciséis (16) a treinta y seis (36) meses cuando la cuantía no exceda de diez (10) salarios mínimos legales mensuales vigentes.

ARTICULO 240. HURTO CALIFICADO. <Artículo modificado por el artículo 37 de la Ley 1142 de 2007. El nuevo texto es el siguiente:> La pena será de prisión de seis (6) a catorce (14) años, si el hurto se cometiere:

(…)

4. Con escalonamiento, o con llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o violando o superando seguridades electrónicas u otras semejantes. (Subrayas fuera del texto original).

Antes de la expedición de la Ley 1273 de 2009, el estatuto sustantivo sancionaba, de esta manera, la modalidad de sustracción de una cosa mueble ajena –el dinero- para provecho propio o de un

tercero a través de la ruptura de las barreras de protección informáticas o electrónicas dispuestas por el titular del bien jurídico del patrimonio económico.

Pero, aprovechando la coyuntura legislativa, que abogaba por la regulación de los delitos informáticos, en el artículo 269I, el legislador quiso redefinir o enriquecer con mayor precisión idiomática, si se quiere, el mecanismo de desplazamiento ilícito de la cosa mueble desde el titular del derecho hacia el sujeto activo, más no creó una nueva acción objeto de juicio de desvalor, porque, se insiste, ella ya estaba tipificada en la conducta simple de hurto y en la circunstancia calificante, al punto que no consagró un nuevo verbo rector sino que, al respecto, se remitió al canon 239 ejusdem y, en función de la pena, al precepto 240 ibidem.

3. Elementos estructurales del tipo penal de hurto por medios informáticos y semejantes desde la dogmática penal.

El texto del artículo 269I que tipifica el delito de hurto por medios informáticos y semejantes es del siguiente tenor:

> El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.

Lo primero a señalar es que, como viene de verse, se trata de un tipo penal de naturaleza claramente subordinada y compuesta. En efecto, la descripción normativa, en su tipo objetivo positivo y en la consecuencia jurídica, no consagra la conducta reprochada, el objeto material, ni la sanción correspondiente, sino que, en cuanto se refiere al comportamiento antijurídico y al referido objeto sobre el que recae la acción prohibida, efectúa un reenvío normativo al tipo base de hurto (artículo 239 de la Ley 599 de 2000) y a la disposición que lo califica (canon 240 ejusdem) para determinar la sanción imponible.

En verdad, el precepto examinado -269I- solamente se ocupa de establecer el sujeto activo indeterminado –no cualificado o común y unisubjetivo - del punible y de consagrar unos específicos ingredientes normativos, que lo identifican como un tipo de medio concreto o, si se quiere, determinado, por cuanto estructura una modalidad o mecanismo específico de desapoderamiento de la cosa mueble ajena, a saber, superar las seguridades informáticas mediante i) la manipulación del sistema informático, la red de sistema electrónico, telemático u otro semejante o ii) la suplantación de una persona ante los sistemas de autenticación y de autorización establecidos.

Y es que la remisión en cuestión al hurto simple, se traduce, en lo fundamental, en la introducción de un elemento descriptivo, esto es, del verbo rector traído desde un tipo autónomo, consistente en el apoderamiento ilícito de un bien mueble ajeno. Es decir, que, para la configuración del injusto, la disposición en estudio, redirige al operador judicial hacia el hurto simple, para integrar una suerte de delito complejo que responde a una relación de estricta dependencia.

Si se redactara de forma inclusiva, el tipo penal de hurto por medios informáticos resultaría de la siguiente manera: el que, superando medidas de seguridad informáticas, se apodere de cosa mueble ajena con el fin de obtener provecho para sí o para otro, manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un individuo ante los sistemas de autenticación y de autorización establecidos, incurrirá en pena de prisión de 6 a 14 años.

Ahora, una lectura apresurada del precepto estudiado podría sugerir, equivocadamente, por supuesto, que la conducta reprochada penalmente es la de superar las seguridades informáticas, caso en el cual el bien jurídico de la protección de la información y los datos estaría en clara correspondencia con la concepción de un único interés superior a tutelar; no obstante, es el legislador el que se ocupó de identificar que el comportamiento objeto de reproche es el señalado en el artículo 239, es decir, el de hurto, realizado, eso sí, ejecutando la acción complementaria, consistente en superar (violentar) las seguridades informáticas a través de cualquiera de las dos formas modales de realización de la conducta reseñadas, como derivaciones del tipo básico.

Agréguese, que dicha remisión al artículo 269I abarca no solo el verbo rector de la conducta de hurto simple, el objeto material –la cosa mueble- y el elemento normativo relativo a la ajenidad del

mismo, sino, también el ingrediente especial subjetivo necesario para su comisión, como lo es, el animus lucrandi o la finalidad o propósito doloso de obtener un provecho o utilidad –propio o en favor de un tercero- de carácter patrimonial.

Se constata así, pues, la categoría no autónoma del injusto de hurto por medios informáticos y semejantes y, por consiguiente, su dependencia directa, necesaria e inescindible con la conducta básica de hurto.

El tipo penal analizado, además de estar supeditado al contenido descriptivo y normativo del hurto simple, es de lesión porque exige el efectivo menoscabo del interés jurídicamente tutelado, que para el caso lo son el patrimonio económico y la seguridad en el tráfico a través de los sistemas informáticos; pero también es de resultado, como quiera que para la consumación del desvalor total del injusto requiere el desapoderamiento del dinero con el subsecuente perjuicio, estimable en términos económicos, para quien tenga la relación posesoria con la cosa.

Igualmente, es de conducta instantánea toda vez que el agotamiento del comportamiento típico se perfecciona cuando la víctima es desposeída de su dinero vulnerando los sistemas de protección informáticos dispuestos para su resguardo.

El sujeto pasivo de la infracción, por su parte, no está expresamente determinado en la norma, aunque es posible inferirlo de la conjunción de los tipos base y subordinado, de tal suerte, que lo será el titular del derecho patrimonial birlado o poseedor del dinero sustraído, que, según el caso, podrá serlo el usuario financiero y/o la persona jurídica que lo custodia, dependiendo de cuál sea la barrera informática, telemática o electrónica comprometida para acceder al circulante.

En efecto, si la defensa informática quebrantada corresponde a algún sistema de autorización o autenticación -clave o password- puesta por el sujeto, éste será la víctima, mientras que si los alterados son los mecanismos de protección implementados por la persona jurídica encargada de resguardar el bien, será ésta la llamada a perseguir su reparación.

En cuanto al objeto, la distinción doctrinal entre objeto jurídico y/o material de protección, obliga a determinar, en el caso concreto, que si bien el delito se ubica dentro del título que protege la información y los datos, el bien material del delito no puede ser otro que la cosa mueble ajena que sufre un apoderamiento por parte de un extraño. Los datos, la información y su contenido solo son manipulados con el fin de obtener un provecho económico por medio de la sustracción irregular de la cosa mueble ajena que se condensa en el dinero.

4. Sobre el bien jurídico tutelado en el delito de hurto por medios informáticos y semejantes

El derecho penal tiene por objeto regular, desde el punto de vista sancionatorio, el comportamiento humano que no se adecua al imaginario colectivo de la sociedad. Es así que, con el propósito de salvaguardar los más caros intereses del conglomerado, el poder punitivo del Estado busca reprimir, desde la coerción normativa (prevención general negativa), todo aquel intento por perturbar la tranquilidad y el bien común y motivar a los ciudadanos para que se abstengan de ignorar sus mandatos (prevención general positiva).

Con ese fin, cada nación ha identificado unos especiales valores, cualidades o bienes objeto de protección jurídica, que responden a un querer mayoritario, visible en las normas de carácter sustancial que describen ciertas acciones u omisiones prohibidas y determinan unas sanciones –restrictivas de la libertad o de otros derechos o pecuniarias- frente a su eventual desacato (prevención especial).

Esos objetos de tutela legal –que en el derecho penal liberal eran escasos y básicos: la vida, el honor, la libertad, la propiedad, entre otros- no son necesariamente estáticos, pues los grupos sociales debidamente establecidos o constituidos en Estados, regidos por sus evoluciones o involuciones de naturaleza política, religiosa, científica, tecnológica, etc., han marcado, desde la llamada sociedad del riesgo (ULRICH BECK), las pautas para determinar qué interés en particular debe ser amparado y la forma de hacerlo.

Una de esas formas es el derecho penal, que al reconocer los objetos jurídicos concretos de protección –individuales o colectivos-, a partir, por supuesto, de referentes con asiento en la realidad,

paralelamente determina cuáles son las actividades de los ciudadanos que merecen ser reprobadas y reprimidas con alguna sanción, a efecto de garantizar la inmutabilidad de cada interés superior.

Y es que los tipos penales solo pueden alcanzar su ámbito de prohibición si verdaderamente afectan un bien jurídico, el cual debe justificar, necesariamente, la lesividad de la conducta, o al menos la dirección u orientación protectora que se le atribuye a la norma.

Así es que, al legislador, en función del principio de representación popular, le corresponde escoger entre la multiplicidad de acciones u omisiones humanas capaces de generar un juicio de desvalor, y consignar, en un estatuto punitivo, el correspondiente mandato de prohibición, de tal forma que se habilite una «relación de disponibilidad del sujeto con el objeto» -en los términos de ZAFFARONI - como elemento de contención del poder punitivo.

Sobre la manera de definir los bienes jurídicos tutelados, la doctrina ha reconocido que, generalmente, el interés jurídico tutelado aparece instituido en los títulos y capítulos que agrupan los delitos, pero, en veces, es el intérprete quien debe identificarlo

Acudiendo a un procedimiento de conjugación de las expresiones literales de los rubros de los títulos y los capítulos, que forman la Parte especial, con el "sentido" de la acción descripta en un determinado tipo (…). Y no pocas veces la forma de la acción indicará que, pese a la localización del bien jurídico enunciado por éste solo indirectamente se corresponde con el protegido según el tipo: por ejemplo, [en Argentina] el delito de violación (…) está inserto entre los "delitos contra la honestidad", pero de su contenido se deduce, sin esfuerzos, que lo que en realidad protege es la "libertad sexual".

A veces ocurre que el tipo comprende más de un bien jurídico (p. ej. En el "secuestro" de una persona para pedir rescate (…) entran en juego los bienes jurídicos de la propiedad y de la libertad); en esos casos la tipicidad de la conducta que se examina (…) dependerá del bien jurídico preponderantemente afectado por la conducta del agente, lo cual será materia de interpretación en cada caso particular.

Es así como, por ejemplo, el legislador colombiano advirtió que algunas formas delincuenciales en el ámbito de la informática, que trascendían, en muchas ocasiones, las fronteras nacionales, no estaban siendo objeto del reproche punitivo requerido, pues o no estaban reguladas o permanecían subsumidas en el ámbito de protección de otras garantías, verbi gratia, la intimidad, razón por la que se dio a la tarea de "crear" -léase reconocer-, la vigencia de un nuevo bien jurídico que, de manera sistemática y específica, recogiera todos aquellos comportamientos dispersos a lo largo y ancho del Estatuto Sustantivo.

De este modo, mediante la Ley 1273 de 2009 "creó" el título VII bis "De la protección de la información y de los datos" y, en él, varios tipos autónomos que tendrían por objeto evitar la lesión de este interés jurídico, como el acceso abusivo a un sistema informático, la interceptación de datos informáticos, el daño informático, el uso de software malicioso, la violación de datos personales, por mencionar algunos; no obstante, al final del trámite legislativo menospreció las consecuencias -no inadvertidas inicialmente por cierto-, de regular dentro de este título conductas subordinadas a otros tipos básicos, como lo es el caso del reato de hurto por medios informáticos y semejantes.

Ciertamente, aunque el legislador fue consciente de la dificultad que comportaba la ubicación del bien jurídico protegido respecto de aquellas acciones antijurídicas reguladas dentro del mentado título, que de manera directa afectaban el patrimonio económico, prefirió atar, de manera antitécnica, como lo aseveró el representante de la Fiscalía, la modalidad de la acción típica prohibida –que es el hurto por medios informáticos- al bien jurídico amparado en el referido título VII bis, que adicionar o modificar las circunstancias modales calificantes del artículo 240 del Código Penal, como hubiera sido lo ideal.

De lo hasta aquí dicho, es posible decantar, con meridiana claridad, que pese a la ubicación sistemática del punible de hurto por medios informáticos y semejantes en el título VII bis del Código Penal, rubricado bajo la denominación de la información y los datos, este bien jurídico resulta ser, para el caso concreto -como lo concibió la exposición de motivos del Proyecto de Ley 042 Cámara-, de naturaleza meramente intermedia, pues el interés superior protegido de manera directa es el patrimonio económico, entendido como ese conjunto de derechos y obligaciones, susceptible de ser valorado en términos económicos, más concretamente, en dinero.

En verdad, nadie podría dudar que el mentado ilícito tiene la virtualidad de lesionar tanto la seguridad y la confianza de las personas naturales y jurídicas en los sistemas informáticos, telemáticos, electrónicos o semejantes, con sus componentes de software y hardware, implementados por las entidades encargadas de custodiar el capital de sus usuarios, como los intereses individuales de contenido económico del titular de la cosa ajena, cuestión que ubica al tipo penal examinado en el contexto de los delitos típicamente pluriofensivos por afectar más de un interés jurídico, el descrito expresamente en la legislación penal codificada –en este caso, el título VII bis- y el que surge de manera remota, pero directa, de la realización de la acción injusta.

Sin embargo, es lo cierto que la afrenta contra el primero de los bienes reseñados –de carácter colectivo-: la información y los datos, es solamente mediata (intermedia), porque solo se vincula con el mecanismo ilícito –de naturaleza informática- de sustracción del dinero que no con el comportamiento prohibido, mientras que el ataque contra el segundo (de orden individual): el patrimonio económico, es inmediato, pues se relaciona con la conducta reprobada misma, o sea, con el desapoderamiento de la cosa ajena en tanto mandato de prohibición final que tutela la relación de dominio o tendencia de una persona con la cosa.

A esta conclusión es fácil llegar si se examina la naturaleza subordinada y compuesta –que no autónoma- del injusto de hurto por medios informáticos respecto del tipo básico de hurto, que lo sitúa en similar lugar descriptivo que el hurto calificado -pues a su pena se remite-, y cuando se indaga el espíritu del legislador que, como se vio, a pesar del propósito general de regular actividades ilícitas estrictamente relacionadas con la afectación de los sistemas informáticos y los datos, utilizó esta oportunidad para precisar algunas de las modalidades de hurto desarrolladas para transgredir las defensas de protección informáticas.

Sobre el carácter intermedio del bien jurídico protegido en la conducta de hurto por medios informáticos y semejantes, la doctrina ha elaborado las siguientes reflexiones:

Se trata, entonces, de los denominados bienes jurídicos intermedios, como lo entendía Tiedemann, quien señalaba como ejemplo de tales intereses el tutelado en el delito de estafa informática, que

estaría constituido por el correcto procesamiento de los datos electrónicos, que es tenido como un instrumento imprescindible de la vida económica moderna, y el patrimonio económico.

La aceptación de este bien jurídico intermedio tiene una gran incidencia en la delimitación e interpretación del injusto típico del delito de hurto por medios informáticos y semejantes. Esto porque si los delitos protectores de un bien jurídico intermedio se caracterizan frente a los simples delitos pluriofensivos de peligro por el hecho de que para su consumación se exige la efectiva lesión de uno de los dos valores que lo conformen, el colectivo o el individual, para poder calificar a aquel delito de hurto como protector de un bien jurídico intermedio hay que aceptar que la conducta típica se dirige a lesionar de manera inmediata un bien jurídico individual, al mismo tiempo que provoca dicha lesión la mediata puesta en peligro de otro valor de índole diversa a la del primero, de carácter colectivo.

En el delito de hurto por medios informáticos y semejantes el bien jurídico intermedio está configurado, de un lado, por el interés en la protección del patrimonio económico, que sería el referente individual, cuya lesión permite, de otro lado, apreciar la puesta en peligro del interés general en la seguridad del tráfico de la información y los datos. Esto debido a que la lesión del patrimonio económico como bien jurídico individual está regulada de manera expresa como una exigencia típica del delito de hurto en el Código Penal colombiano; lo cual conduce a la conclusión de que el patrimonio económico sería el referente individual del bien jurídico intermedio.

Al tenerse al delito de hurto por medios informáticos y semejantes como un delito protector de valores supraindividuales, su estructura ha de consistir en que la conducta se encamina a causar la inmediata lesión de un bien jurídico de naturaleza individual (el patrimonio), y ocasiona, además la mediata y abstracta puesta en peligro de otro bien jurídico de naturaleza colectiva (el correcto funcionamiento de los sistemas de información y datos).

Siendo ello así, natural es concluir, como lo hiciera la demandante y el representante del ente acusador, que el tipo penal de hurto por medios informáticos y semejantes no solo está circunscrito al ámbito de punibles contra la información y los datos, sino, esencialmente a la esfera de los lesivos del patrimonio económico, pues es el valor ético jurídico que al final resultaría atacado con la

sustracción de dineros a través de mecanismos ilícitos de manipulación de los sistemas informáticos, electrónicos, telemáticos o similares, o suplantación de las personas ante los sistemas de autenticación y de autorización.

5. Alcance de la figura de reparación integral frente al delito de hurto por medios informáticos y semejantes.

La reparación integral, consagrada en el artículo 269 de la Ley 599 de 2000, que tiene su antecedente en el artículo 374 del Decreto Ley 100 de 1980, es un derecho, que no un beneficio , consistente en una reducción de la mitad a las tres cuartas partes de la pena en favor de quien hubiere sido condenado por delitos contra el patrimonio económico, siempre que haya restituido el objeto material del delito o su valor, e indemnizare los perjuicios ocasionados al ofendido o perjudicado, antes del fallo de primera o única instancia.

Para mayor claridad, es oportuno puntualizar que la norma en cuestión, expresamente, delimita la posibilidad de reconocer esta garantía respecto de «las penas señaladas en los capítulos anteriores», refiriéndose con ello a los delitos consagrados en los capítulos I al VIII del Título VII del Código Penal, lo cual podría sugerir, en sentido literal, que única y exclusivamente los injustos allí reglados son los llamados a ser objeto de tal descuento legal.

Con todo, es lo cierto que en vigencia del Estado constitucional y democrático de derecho, una interpretación sistemática e integradora del estatuto punitivo, garante de los valores de justicia e igualdad jurídica ante la ley, permite concluir que si todos esos capítulos regulan ilícitos contra el patrimonio económico, porque a ese bien jurídico se contraen, de acuerdo con la denominación del Título VII al que pertenecen, igualmente, el delito de hurto por medios informáticos y semejantes debería ser susceptible de idéntica consecuencia legal, es decir, del descuento por reparación integral, sobre todo porque, como fue ampliamente discernido atrás, la conducta reprochada: apoderamiento, el objeto material –la cosa mueble-, el elemento normativo concerniente a la ajenidad del mismo y la pena, sí están descritos en el capítulo I del aludido título (artículos 239 y 240 ejusdem).

En todo caso, si fuera necesario, también podría involucrarse el concepto de analogía en bonam partem , el cual únicamente es admisible, en el ámbito penal «en materias permisivas», a voces del inciso 3º del artículo 6º de la Ley 599 de 2000.

Esto, teniendo en consideración que, como quedó visto, el interés jurídico inmediato de protección en ese reato es, justamente, de orbe patrimonial, en la medida que corresponde a un tipo penal subordinado respecto del tipo básico de hurto.

Ahora, lo recién argumentado, no pretende sostener la idea categórica de que el tipo penal de hurto por medios informáticos es necesariamente análogo al de hurto calificado, pues, como resulta obvio, éste no está dentro de la esfera de protección de la información y los datos o la intimidad, como si lo está el punible que nos ocupa; pero lo que sí se encuentra sujeto al criterio analógico, en cuanto resulta ser benigno al procesado, es la posibilidad de otorgar a un supuesto de hecho similar (protección del bien del patrimonio económico), la misma consecuencia jurídica que le imprime el artículo 269 ejusdem a los delitos rubricados bajo los capítulos comprendidos en el Título VII.

Esta postura es compatible y fiel al interés del legislador por entregar una ventaja punitiva a aquel que repare en términos económicos el daño causado por delitos que agredan el patrimonio de las personas.

6. El caso concreto

Como desde el inicio se anticipó, el problema jurídico determinante, en el asunto de la especie, se contrae a establecer si los jueces de instancia incurrieron en violación directa de la ley sustancial por interpretación errónea del artículo 269I de la Ley 599 de 2000 con la consecuente falta de aplicación del canon 269 ejusdem.

La respuesta es decididamente afirmativa, pues se constata que, de espaldas a la estructura dogmática del delito de hurto por medios informáticos y al interés tutelar que tuvo el órgano legislativo al consagrar dicho tipo penal, los falladores inaplicaron la rebaja punitiva por reparación integral, pese a que el sentenciado acreditó el cumplimiento de todos los requisitos de orden legal para ser beneficiario de la misma, como adelante se demostrará.

Al efecto, varias fueron las razones de los jueces de instancia, pero, como se examinará, ninguna de ellas tiene verdadero fundamento jurídico.

De un lado, el juez de primer nivel adujo, con apoyo en el auto CSJ AP 13 sep. 2011, rad. 37.145, según el cual «la citada diminuente sólo es aplicable a los delitos que atentan contra el patrimonio económico, y no aquél que propende por la protección de la información y los datos», que «la redacción normativa y la ubicación sistemática del tipo penal que define el delito de hurto por medios informáticos y semejantes indican que no protege el patrimonio económico, sino bienes de naturaleza diversa, vale decir, (…) la información y los datos (…)» .

Resaltó, asimismo, el a quo que la Corte en auto CSJ AP, 14 ag. 2012, rad. 39.160, señaló que cuando el artículo 269 de la Ley 599 de 2000 incluye la expresión "las penas señaladas en los artículos anteriores", se está refiriendo a que su ámbito de aplicación es única y exclusivamente el Título VII del estatuto sustantivo, esto es, los delitos contra el patrimonio económico.».

Y remató sosteniendo que esta Corporación definió que en el delito de "hurto de hidrocarburos" no cabe la aplicación del artículo 269 ibidem porque el bien jurídico protegido no es el del patrimonio económico, dado su carácter de tipo penal autónomo, criterio que en sentir del juzgador debe ser empleado respecto del punible de hurto por medios informáticos -postura que también comparte el ad quem-.

Al respecto, basta señalar que, tal como lo pusiera en evidencia la casacionista y lo destacara el representante de la Fiscalía, los precedentes jurisprudenciales empleados por el juez de primer nivel resultan del todo impertinentes y descontextualizados, de cara al caso de la especie.

Ciertamente, de una parte, cuando esta Sala de Casación Penal aseguró, en el proveído CSJ AP 13 sep. 2011, rad. 37.145, que la rebaja por reparación integral era imposible frente a los punibles previstos en el Título VII bis, en tanto estaban destinados a proteger la información y el dato y el derecho a la intimidad, lo expresó, concretamente, en torno al injusto de violación de datos personales,

agravado, conducta claramente autónoma –no subordinada- y efectivamente lesiva de los referidos intereses jurídicos y no del patrimonio económico.

De igual manera, la reflexión de esta Corporación, en el sentido que los únicos delitos que admiten la rebaja por reparación integral son los del Título VII del Código Penal, esto es, los lesivos del patrimonio económico, si bien es consistente con el entendimiento básico del mentado artículo 269, no fue bien entendida por el fallador de primer grado, pues no se percató de que, en el caso examinado por la Corte, la pretensión de descuento punitivo por reparación integral se negó porque los reatos por los que allí se procedía eran los de proxenetismo con menor de edad y utilización o facilitación de medios de comunicación para ofrecer actividades sexuales con personas menores de dieciocho años, infracciones que, en modo alguno, gozan de algún contenido patrimonial que debiera ser salvaguardado.

Nótese, cómo la Sala de Casación Penal precisa en la providencia citada por el juzgador (CSJ AP, 14 ag. 2012, rad. 39.160) al respecto lo siguiente:

> Como bien lo señaló el representante del Ministerio Público en la audiencia oral de sustentación, ello es una manifestación de la política criminal del Estado, en la cual la afectación del bien jurídico que con la conminación de pena el legislador pretende proteger merece de manera significativa un menor grado de reproche, "si antes de dictarse sentencia de primera o única instancia el responsable restituyere el objeto material del delito, o su valor, e indemnizare los perjuicios ocasionados al ofendido o perjudicado".

En los delitos sexuales, por el contrario, el objeto de protección no son los bienes muebles o fungibles que tenga o posea una persona, sino la persona misma, en particular, el derecho a tener una formación apropiada en materia sexual, a no ser explotado por otros en ese sentido, a no ser sometido a abusos ni maltratos de tal índole, etcétera. (Subrayas fuera del texto original).

Ahora, del hecho que el ilícito de apoderamiento de hidrocarburos esté referenciado al ámbito de los injustos contra el orden económico y social –cuestión admitida por la Corte-, no se sigue que el delito que nos ocupa no se adscriba a los punibles contra el patrimonio económico.

En verdad, el objeto material del primero de ellos recae en los hidrocarburos y sus derivados biocombustibles o mezclas que los contengan debidamente reglamentados, cuando sean transportados a través de un oleoducto, gasoducto, poliducto o a través de cualquier otro medio, o cuando se encuentren almacenados en fuentes inmediatas de abastecimiento o plantas de bombeo y la conducta reprochada está claramente individualizada en un tipo de naturaleza autónoma, mientras que en el segundo, la acción típica se integra con los tipos base y subordinado y tanto ella como su objeto material no corresponden a la defraudación de un sustrato económico de la nación sino al interés económico particular, máxime, si se recuerda que equivale, más a una modalidad de la acción prohibida que al comportamiento antijurídico en sí mismo considerado.

En todos los casos, resultaba, por decir lo menos, desafortunado asimilar las razones esgrimidas por la Corte para negar la reparación integral frente a tan puntuales infracciones penales con el supuesto jurídico examinado.

Las consideraciones del Tribunal, por su lado, adolecen de similares defectos hermenéuticos sustantivos.

Nótese sobre el particular, cómo, aunque para desentrañar el sentido de la norma estudiada (artículo 269I) el ad quem se valió del informe de ponencia para primer debate a los proyectos acumulados –no precisa si en Senado o en Cámara- que indica que la intención del Congreso era amparar el bien jurídico de la información y los datos, en su análisis sesgado pasó por alto lo argumentado por los parlamentarios en el resto del trámite legislativo, en el sentido que su pretensión también era tutelar el patrimonio económico de los usuarios azotados por el flagelo del hurto a través de las nuevas tecnologías, al punto que advirtieron sobre la naturaleza apenas intermedia del aludido bien jurídico.

A dicha falencia interpretativa, debe sumársele la derivada de admitir, contrariando el principio de no contradicción, que algunas de las conductas consagradas en el Título VII bis, como el hurto por medios informáticos, son pluriofensivas, pero aun así no es posible aplicar la mencionada rebaja del canon 269 porque ella solamente cabe respecto de los delitos de aquella sección del Código, según lo expresó la Corte frente al injusto de violación de datos personales.

Este razonamiento del juez plural, evidentemente restrictivo, parte de asimilar, como si fuera posible, el injusto recién mencionado con el de hurto por medios informáticos, de estructura dogmática sustancialmente diferente, y de tener como autónomo un tipo penal que, si bien es nuevo, está en definitiva subordinado al tipo base de hurto -en tanto, stricto sensu, constituye una modalidad más de ese clásico punible- y a la pena del hurto calificado.

Por manera que, resulta diáfano el quebranto inmediato de la ley sustancial, por conducto de una deficiente interpretación del artículo 269I del Código Penal, que derivó en la exclusión evidente del canon 269 ejusdem, la cual tiene incidencia determinante en el sentido del fallo impugnado, en tanto, como enseguida se constatará, el procesado satisface todos los requisitos establecidos en orden al reconocimiento del derecho a un descuento de la mitad a las tres cuartas partes de la pena.

7. Verificación de los requisitos de la figura de la reparación integral.

El canon 269 de la Ley 599 de 2000, bajo la interpretación consignada en esta providencia, demanda, para la concesión de la rebaja por reparación integral, el cumplimiento de los siguientes presupuestos:

i) El delito objeto de condena debe estar consagrado entre los capítulos I al VIII del Título VII del Código Penal o, en todo caso, atentar contra el patrimonio económico.

ii) El responsable de la infracción penal está obligado a restituir el objeto material del delito o su valor, e indemnizar los perjuicios ocasionados al ofendido o perjudicado.

Significa lo anterior que, debe existir una reparación de orden económico, equivalente al valor del daño causado, lo cual se puede alcanzar por dos vías devolviendo el objeto material del ilícito o su equivalente junto con el resarcimiento de los perjuicios causados con la infracción, o satisfaciendo estos últimos, cuando quiera que no fuera exigible o posible la restitución del aludido objeto material (CSJ AP, 22 may. 2013, rad. 38.628).

iii) La reparación tiene que surtirse, necesariamente, antes de que se dicte sentencia de primera o única instancia.

En el asunto que nos convoca, se tiene que, si bien el delito de hurto por medios informáticos y semejantes no está consagrado entre los delitos de que trata el Título VII de la Ley 599 de 2000, como quedó ampliamente demostrado a lo largo de la providencia, no solo atenta contra el bien jurídico del patrimonio económico, sino que la descripción típica esencial está –es decir, la conducta, el objeto material y la pena- está regulado en los cánones 239 y 240 del Código Penal.

Así también, obra constancia en el expediente de que el representante de la víctima (Incocrédito) manifestó durante las diligencias de preacuerdo y verificación del mismo ante el juez de conocimiento e, incluso, en sede de casación, que dicho interviniente había sido reparado integralmente por los procesados.

En efecto, en el acta de preacuerdo se lee lo siguiente:

Se advierte por parte de Incocrédito que DIEGO MAURICIO ARIAS, ha reintegrado a la cuenta de Davivienda a nombre de Incocrédito el valor de cuatro millones ciento sesenta mil trescientos noventa pesos ($4.160.390.oo) y por parte de RICARDO JAIME SÁNCHEZ CASTRILLÓN, HA REINTEGRADO a la cuenta del Banco Davivienda a nombre de Incocrédito, cuenta que fue establecida por Davivienda para el reintegro de dinero por operaciones fraudulentas la suma de tres millones noventa y ocho mil cuatrocientos noventa pesos ($3.098.490.oo). De esta manera, como incredito (sic) advertimos que ha existido por parte de los señores RICARDO JAIME SANCHEZ (sic) CASTRILLON (sic) y DIEGO MAURICIO ARIAS IBAÑEZ (sic), indemnización integral por los perjuicios ocasionados con los hechos delictivos sucedidos el pasado 7 de Diciembre de 2012, en los establecimientos comerciales Múcura y Tennis y Tennis.- Adjuntamos la documentación de los extractos o soportes que se advierten en este documento.

Durante la audiencia de legalización del preacuerdo reiteró que no tenía ninguna objeción frente al mismo, considerando que los extractos de unas notas débito cargadas a los establecimientos Múcura

y Tennis & Tennis y la consignación del saldo que había quedado pendiente por las transacciones fraudulentas .

Y en la audiencia de sustentación oral del recurso de casación, recalcó que el acusado indemnizó integralmente a las entidades financieras por su participación en las conductas punibles a él endilgadas, particularmente, en la clonación de tarjetas en los establecimientos comerciales y la respectiva defraudación.

En este punto, es imperioso precisar que aunque el procesado no fue el sujeto que indemnizó integralmente a la víctima, es viable reconocer en su favor el descuento solicitado, habida cuenta que, de tiempo atrás, la jurisprudencia, de manera pacífica, ha reiterado que la rebaja por reparación integral se puede hacer extensiva a los copartícipes y, en este caso, se observa que fueron los administradores de los establecimientos comerciales (coautores) comprometidos en la falsificación de las tarjetas de crédito y en las transacciones fraudulentas quienes retornaron a la entidad perjudicada las sumas de las que se habían apoderado.

Finalmente, es nítido que dicha reparación integral se produjo antes de que se emitiera el fallo de primer grado del 19 de diciembre de 2013, concretamente, el 14 de febrero de igual año , esto es, el día en que las partes –procesado y Fiscalía- suscribieron el preacuerdo.

Siendo lo anterior así, y estando acreditada la infracción directa denunciada por la defensa, hay lugar a casar parcialmente la sentencia para reconocer la rebaja de pena por reparación integral demandada respecto del delito de hurto por medios informáticos y semejantes, agravado.

7. La redosificación punitiva

CARLOS ARTURO ÁLVAREZ TRUJILLO fue condenado en calidad de coautor del delito de hurto por medios informáticos y semejantes, agravado, en concurso con los de concierto para delinquir y falsedad en documento privado (artículos 269I, 269H.1, 340 y 268 del Código Penal), a la pena de 92 meses y 12 días de prisión.

Para llegar a este número, por el primero de los punibles mencionados (base), el juzgador le impuso el mínimo de 108 meses de prisión, por el segundo, 48 meses y, por el tercero, 12 meses, para un total preliminar de 168 meses, cantidad a la que le dedujo un 45% por razón del preacuerdo, quedando en definitiva en 92 meses y 12 días.

Ahora, para restablecer el derecho conculcado por las instancias al procesado, la Corte estima procedente reconocer un descuento por reparación integral (artículo 269 ejusdem) de la mitad de la pena impuesta por el delito de hurto por medios informáticos y semejantes, considerando que la reparación integral no se produjo en la primera fase procesal (imputación), sino algún tiempo después y que la conducta de defraudación de los usuarios del sistema financiero a través de canales informáticos, desplegada por el acusado, en concurso criminal con varios sujetos, reviste especial connotación, tornando necesario dar alcance a los principios de prevención general y especial.

Esa proporción, aplicada a los 108 meses de prisión por el mentado injusto, equivale a 54 meses , que sumados a los 48 y 12 meses por los demás delitos concursantes, arroja un resultado de 114 meses .

Ahora, como quiera que este valor excede el otro tanto de la pena individualmente considerada para el injusto de hurto por medios informáticos, conforme al artículo 31 del Código Penal, la sanción por los reatos concursantes se reducirá estrictamente al doble de 54 meses, para un monto de 108 meses, cantidad a la que corresponde rebajar un 45% (48.6 meses) en los términos del preacuerdo, para un monto definitivo de 59,4 meses o, lo que es igual 59 meses y 12 días.

A dicha cantidad, también, deberá reducirse la sanción accesoria de inhabilitación para el ejercicio de derechos y funciones públicas.

8. Sobre los mecanismos sustitutivos de la prisión.

Como quiera que, como acaba de verse, el monto de pena impuesto al sentenciado varió con ocasión de la redosificación punitiva, se impone revisar de nuevo si él podría tener derecho a la suspensión condicional de la ejecución de la pena o a la prisión domiciliaria.

8.1 Al respecto, en punto del subrogado, lo primero a destacar es que, de acuerdo con la normas vigentes al tiempo de los hechos -7 de diciembre de 2012- (artículo 63 y 38 del Código Penal, sin las modificaciones introducidas por la Ley 1709 de 2014) no es viable la concesión del subrogado o del sustituto penal, pues el factor objetivo lo impide, habida cuenta que para el primero, el precepto exige que la pena de prisión impuesta no exceda de 3 años y para el segundo que la sentencia se imponga por conducta punible cuya pena mínima prevista en la ley sea de 5 años o menos y, en el asunto de la especie, se tiene que CARLOS ARTURO ÁLVAREZ TRUJILLO fue condenado a la sanción de 59 meses y 12 días de sanción aflictiva de la libertad y el monto mínimo sancionatorio previsto para el injusto de hurto por medios informáticos y semejantes, agravado, es de 108 meses, ambas cantidades superiores a los topes legales mencionados.

En similar sentido, el ejercicio de favorabilidad, que resulta de la aplicación de la Ley 1709 de 2014, muestra que tampoco ésta regulación permite la concesión de alguno de los mentados derechos.

8.2. En efecto, el artículo 63 del Código Penal, modificado por el artículo 29 de la Ley 1709 de 2014, enumera los siguientes requisitos para ser beneficiario de la suspensión condicional de la ejecución de la pena:

1. Que la pena impuesta sea de prisión que no exceda de cuatro (4) años.

2. Si la persona condenada carece de antecedentes penales y no se trata de uno de los delitos contenidos el inciso 2o del artículo 68A de la Ley 599 de 2000, el juez de conocimiento concederá la medida con base solamente en el requisito objetivo señalado en el numeral 1 de este artículo.

3. Si la persona condenada tiene antecedentes penales por delito doloso dentro de los cinco (5) años anteriores, el juez podrá conceder la medida cuando los antecedentes personales, sociales y familiares del sentenciado sean indicativos de que no existe necesidad de ejecución de la pena.

En el caso examinado, la sanción definitivamente impuesta al procesado (59 meses y 12 días) es superior a los cuatro (4) años que el legislador determinó como presupuesto objetivo para acceder al

referido subrogado; por ende, no es necesario avanzar en la evaluación de los demás requisitos y, por supuesto, a su reconocimiento.

Ahora, a manera de obiter dicta, no sobra aclarar que de haber satisfecho el procesado dicho requerimiento objetivo, no habría sido posible negarle la condena de ejecución condicional con fundamento en el artículo 68A -que prohíbe la concesión de este beneficio a quienes sean condenados por el reato de hurto calificado- y aduciendo, para el efecto, la similitud dogmática del delito de hurto por medios informáticos con el descrito en el artículo 240 ibidem, toda vez que, aunque atrás, en punto de la reparación integral, se utilizó el criterio analógico para conferir igual consecuencia jurídica a un mismo supuesto de hecho, no sería viable argumentar algo semejante en sentido desfavorable a los intereses del procesado, pues la analogía en malam partem está proscrita en materia penal (artículo 6º, inciso 3º del Código Penal).

8.3. Por su parte, el canon 38B ejusdem establece que son requisitos para conceder la prisión domiciliaria que i) la sentencia se imponga por un delito cuya pena mínima prevista en la ley sea de ocho (8) años de prisión o menos, ii) no se trate de uno de los delitos incluidos en el inciso 2º del canon 68A de la Ley 599 de 2000, iii) se demuestre el arraigo familiar y social del condenado y iv) se garantice mediante caución el cumplimiento de las obligaciones consagradas en el numeral 4º de la norma.

Trasladando estos enunciados al asunto examinado, se observa que uno de los delitos por el que fue condenado ÁLVAREZ TRUJILLO –hurto por medios informáticos y semejantes- no satisface el presupuesto objetivo, habida cuenta que la pena mínima para dicho delito está prevista en 108 meses y el precepto en cuestión exige que la sanción a imponer sea igual o inferior a 8 años. Por modo que, por esta razón, tampoco es posible la sustitución de la pena aflictiva de la libertad en establecimiento carcelario al domicilio.

En mérito de lo expuesto, la Sala de Casación Penal de la Corte Suprema de Justicia, administrando justicia en nombre de la República y por autoridad de la ley,

RESUELVE

Primero. Casar parcialmente la sentencia proferida el 29 de agosto de 2013 por la Sala Penal del Tribunal Superior de Neiva, en el sentido de reconocer a favor de CARLOS ARTURO ÁLVAREZ TRUJILLO la rebaja por reparación integral, de que trata el artículo 269 del Código Penal.

En consecuencia, fijar la pena de prisión en 59 meses y 12 días, mismo término al que se reduce la sanción accesoria de inhabilitación para el ejercicio de derechos y funciones públicas.

Segundo. Negar la suspensión condicional de la ejecución de la pena y la prisión domiciliaria, conforme a las razones expuestas en la parte motiva de esta providencia.

En lo demás, el fallo permanece incólume.

Tercero. Contra esta decisión no procede recurso alguno.

Notifíquese y cúmplase

JOSÉ LUIS BARCELÓ CAMACHO
Presidente

JOSÉ LEONIDAS BUSTOS MARTÍNEZ

FERNANDO ALBERTO CASTRO CABALLERO

EUGENIO FERNÁNDEZ CARLIER

MARÍA DEL ROSARIO GONZÁLEZ MUÑOZ

GUSTAVO ENRIQUE MALO FERNÁNDEZ

EYDER PATIÑO CABRERA

PATRICIA SALAZAR CUÉLLAR

LUIS GUILLERMO SALAZAR OTERO

NUBIA YOLANDA NOVA GARCÍA

Secretaria

ANEXO 3: Normativa RFC 3227

Red Grupo de Trabajo D. Brzezinski
Petición de Comentarios: 3227 In-Q-Tel
BCP: 55 T. Killalea
Categoría: Mejor práctica actual neart.org

Directrices para la Evidencia de archivo y colección

Estado de este documento

Este documento especifica un Internet Mejores Prácticas Actuales de la comunidad de Internet, y solicita debate y sugerencias para mejoras. La distribución de este memo es ilimitada.

Aviso de copyright

Abstracto

Un "incidente de seguridad" como se define en el "Glosario de Seguridad de Internet", RFC 2828, es un evento del sistema relevante para la seguridad en el que el sistema de política de seguridad se desobedece o violada de otro modo. El propósito de este documento es proporcionar a los administradores de sistemas con las directrices sobre la recopilación y el archivo de las pruebas pertinentes para un valor tal incidente.

Si la recopilación de pruebas se hace correctamente, es mucho más útil en aprehender el atacante, y se destaca una mayor posibilidad de ser admisible en el caso de un proceso judicial.

Tabla de contenido

1. Introducción

Un "incidente de seguridad" como se define en [RFC2828] es un pertinentes para la protección de eventos del sistema en el que se desobedece la política de seguridad del sistema o infringido de otro modo. El propósito de este documento es proporcionar los administradores del sistema con directrices sobre la recopilación y el archivo de las pruebas correspondientes a un incidente de este tipo de seguridad. No es nuestra intención de insistir en que todos los administradores del sistema rígidamente seguir estas directrices cada vez que tienen un incidente de seguridad. Más bien,

queremos proporcionar orientación sobre lo que deben hacer si eligen recoger y proteger la información relativa a una intrusión.

Tal colección representa un esfuerzo considerable por parte del Administrador de sistema. Se han hecho grandes progresos en los últimos años para acelerar la re-instalación del sistema operativo y de facilitar la reversión de un sistema a un estado "conocido", lo que hace la "opción fácil" aún más atractivo. Mientras tanto, poco se ha hacer para proporcionar formas fáciles de pruebas archivado (la difícil opción). Además, el aumento de las capacidades de disco y de memoria y más uso generalizado de sigilo y cubrirse las pistas tácticas por los atacantes han agravado el problema.

Si la recopilación de pruebas se hace correctamente, es mucho más útil en aprehender el atacante, y se destaca una mayor posibilidad de ser admisible en el caso de un proceso judicial.

Debe utilizar estas directrices como base para la formulación de su los procedimientos de toma de muestras del sitio, y deben incorporar su los procedimientos del sitio en su Manejo de Incidentes documentación. Los directrices de este documento pueden no ser apropiados bajo todas jurisdicciones. Una vez que haya formulado la evidencia de su sitio procedimientos de recogida, usted debe tener aplicación de la ley para su jurisdicción confirmar que son adecuadas.

1.1 Convenciones utilizadas en este documento

Las palabras clave "REQUERIDO", "DEBE", "NO DEBE", "DEBERÍA", "NO DEBE", y "MAYO" En este documento se han de interpretar como se describe en "Key palabras para su uso en RFC para Indicar Niveles de exigencia "[RFC2119].

2 Principios rectores durante la recolección de evidencia

- Se adhieren a la política de seguridad de su sitio y activar el Manejo adecuado de incidentes y el personal de aplicación de la ley.
- Captura como una imagen precisa del sistema como sea posible.

- Mantener notas detalladas. Estos deben incluir las fechas y horas. Si posible generar una transcripción automática. (Por ejemplo, en Unix sistemas del programa de "guión" se puede utilizar, sin embargo, la salida del archivo que genera no debe ser a medios de comunicación que es parte de la evidencia). Notas y documentos de impresión deben estar firmadas y fechadas.

- Tenga en cuenta la diferencia entre el reloj del sistema y UTC. Para cada marca de tiempo, indicar si se utiliza UTC o en hora local.

- Esté preparado para testificar (quizás años más tarde) que detalle todas acciones que tomaron y en qué momento. Las notas detalladas serán vital.

- Reducir al mínimo los cambios en los datos a medida que se está recogiendo. Esto es no se limitan a cambios en el contenido; se debe evitar el archivo de actualización o tiempos de acceso de directorio.

- Retirar las vías externas para el cambio.

- Cuando se enfrenta a una elección entre la recolección y análisis que debe hacer primero y recogida posterior análisis.

- A pesar de que casi no necesita afirmar, sus procedimientos deben ser implementable. Al igual que con cualquier aspecto de la respuesta a un incidente políticas, procedimientos debe ser probado para asegurar la viabilidad, particularmente en una crisis. Si es posible, deben aplicarse procedimientos automatizado por razones de velocidad y precisión. Ser metódico.

- Para cada dispositivo, un enfoque metódico, que debe adoptarse sigue las directrices establecidas en el procedimiento de recogida. La velocidad será a menudo crítico así que donde hay una serie de dispositivos que requieren un examen puede ser apropiado para difundir el trabajo entre su equipo para recoger las pruebas en paralelo. Sin embargo en una sola colección sistema dado debe hacerse paso Por paso.

- Desplazarse desde la volátil para el menos volátil (véase la Orden La volatilidad de abajo).

- Debe hacer una copia de nivel de bits de los medios de comunicación del sistema. Si tu desean hacer el análisis forense, debe realizar una copia de nivel de bits de su evidencia copiar para tal fin, ya que su análisis es casi seguro que variar los horarios de acceso a archivos. Evitar hace medicina forense en la copia de la evidencia.

2.1 Orden de volatilidad

Cuando la recogida de pruebas se debe proceder de la volatilidad a la menos volátil. He aquí un ejemplo de orden volatilidad para un típico sistema.

- Registros, caché
- Estadísticas de la tabla de enrutamiento, caché ARP, la tabla de procesos, del núcleo, memoria
- sistemas de archivos temporales
- disco
- El registro remoto y los datos de seguimiento que es relevante para la sistema en cuestión
- Configuración física, la topología de red
- Medios de archivado

2.2 Las cosas para evitar

Es muy fácil de destruir pruebas, aunque inadvertidamente.

- No apague hasta que haya completado la recopilación de pruebas. Hay mucha evidencia que se puede perder y el atacante puede haber alterado el inicio / scripts de apagado / servicios para destruir pruebas.

- No confíe en los programas en el sistema. Ejecutar sus pruebas programas de recolección de los medios de comunicación debidamente protegidas (véase abajo).

- No ejecute programas que modifican el tiempo de acceso de todos los archivos del sistema (por ejemplo, "alquitrán" o "xcopy ').

- Al retirar las vías externas para el cambio que se nota simplemente desconectar o filtrado de la red puede desencadenar "interruptores" hombre muerto que detectan cuando están fuera de la red y limpie pruebas.

2.3 Consideraciones sobre la privacidad

- Respetar las normas y directrices de privacidad de su empresa y su jurisdicción legal. En particular, asegurarse de que nadie la información recopilada junto con la evidencia que está buscando para el que está disponible para cualquier persona que normalmente no tendrían acceso a esta información. Esto incluye el acceso a los archivos de registro (que pueden revelar patrones de comportamiento de los usuarios), así como los datos personales archivos.

- No entrometerse en la privacidad de las personas que no tienen fuertes justificación. En particular, no recoger la información de áreas que normalmente no tienen razón para el acceso (por ejemplo, almacenes de archivos personales) a menos que tenga suficiente indicación que no es un verdadero incidente.

- Asegúrese de que tiene el respaldo de su empresa de establecidos procedimientos de adopción de las medidas que hacen para recoger evidencia de un incidente.

2.4 Consideraciones legales

La prueba informática necesita ser

- Admisible: Se debe cumplir con ciertas normas legales que se le han puede ser puesto ante un tribunal.
- Auténtico: Debe ser posible para atar positivamente probatorio el material con el incidente.
- Completa: Se debe contar toda la historia y no sólo una en particular perspectiva.
- Fiabilidad: No debe haber nada acerca de cómo era la evidencia recogido y posteriormente manipulado que arroja dudas sobre su autenticidad y veracidad.
- Creíble: Debería ser fácilmente creíble y comprensible por un tribunal.

3 El Procedimiento de Recogida

Sus procedimientos de recolección deben ser lo más detallado posible. Como es en el caso de los procedimientos generales de gestión de incidentes, que deberían ser inequívoca, y debe minimizar la cantidad de toma de decisiones sea necesario durante el proceso de recolección.

3.1 Transparencia

Los métodos utilizados para recoger pruebas deben ser transparentes y reproducible. Debe estar preparado para reproducir con precisión los métodos que utilizó, y has probado a los métodos por los independientes expertos.

3.2 Pasos Collection

- ¿Dónde está la evidencia? Lista de lo que los sistemas estaban involucrados en el incidente y de la que se recogerá la evidencia.
- Establecer lo que es probable que sea relevante y admisible. Cuando en caso de duda errar por el lado de la recogida de exceso en lugar de no suficiente.
- Para cada sistema, obtener la orden correspondiente de la volatilidad.
- Retirar las vías externas para el cambio.
- Tras el fin de la volatilidad, recoger las pruebas con herramientas como se discute en la Sección 5.
- Registrar el grado de sincronización del reloj del sistema.
- La pregunta ¿qué otra cosa puede ser una prueba a medida que trabaja a través de la pasos de recogida.
- Documento de cada paso.
- No se olvide de las personas involucradas. Tome nota de que estaba allí y ¿qué estaban haciendo, lo que observaron y cómo reaccionado.

Cuando sea factible debe tener en cuenta la generación de sumas de comprobación y firmar criptográficamente las pruebas recogidas, ya que esto puede hacer que sea más fácil de conservar una fuerte cadena de evidencia. En tal caso, deberá no modifican las pruebas.

4 El procedimiento de archivo

La evidencia debe ser estrictamente asegurada. Además, la cadena de custodia debe estar claramente documentado.

4.1 Cadena de Custodia

Usted debe ser capaz de describir claramente cómo se encontró la evidencia, la forma en que se manejó y todo lo que pasó con él.

La siguiente necesidad de documentarse

- ¿Dónde, cuándo y por quién fue la evidencia descubierta y recogido?
- ¿Dónde, cuándo y por quién fue la evidencia manejado o examinada?
- ¿Quién tenía la custodia de las pruebas, durante qué período. Cómo fue se almacena?
- Cuando la evidencia cambió la custodia, cuándo y cómo se hizo la transferencia se produce (se incluyen los números de envío, etc.).

4.2 ¿Dónde y cómo archivar?

Si es posible, los medios de comunicación de uso común (en lugar de algunos de almacenamiento oscura medios de comunicación) se debe utilizar para el archivo.

El acceso a las pruebas debe ser muy restringido, y debe ser claramente documentada. Debe ser posible detectar no autorizado acceso.

5 herramientas que necesitará

Debe tener los programas que hay que hacer la recopilación de pruebas y forense en medios de sólo lectura (por ejemplo, un CD). Debe haber preparado tal conjunto de herramientas para cada uno de los sistemas operativos que administra antes de tener que usarlo.

Su conjunto de herramientas debe incluir lo siguiente:

- Un programa para el examen de los procesos (por ejemplo, 'p').

- programas para examinar el estado del sistema (por ejemplo, '', showrev, 'Ifconfig', 'netstat', 'arp').

- Un programa para hacer copias de bit a bit (por ejemplo, 'DD', 'SafeBack').

- programas para la generación de sumas de comprobación y firmas (por ejemplo, 'Sha1sum', un 'dd' suma de control habilitados, 'SafeBack', 'PGP').

- programas para la generación de imágenes del núcleo y para examinarlas (Por ejemplo, 'gcore', 'gdb').

- Secuencias de comandos para automatizar la recopilación de pruebas (por ejemplo, el forense de Toolkit [FAR1999]).

Los programas en su conjunto de herramientas deben ser enlazados estáticamente, y no debe requerir el uso de las bibliotecas de otros que los medios de sólo lectura. Incluso entonces, desde rootkits modernos se pueden instalar a través de módulo de núcleo, se debe considerar que sus herramientas no podría ser que le da una imagen completa del sistema.

Usted debe estar preparado para dar fe de la autenticidad y fiabilidad de las herramientas que se utilizan.

6 Referencias

[FAR1999] Farmer, D., y W Venema, "Análisis de la informática forense Folletos de clase ", http://www.fish.com/forensics/

[RFC2119] Bradner, S., "Palabras clave para su uso en RFC para Indicar Niveles de exigencia ", BCP 14, RFC 2119, marzo de 1997.

[RFC2196] Fraser, B., "Manual de Seguridad del sitio", FYI 8, RFC 2196, Septiembre de 1997.

[RFC2350] Brownlee, N. y E. Guttman, "Las expectativas para el ordenador Incidentes de Seguridad ", FYI 8, RFC 2350, junio de 1998.

[RFC2828] Shirey, R., "Internet Glosario de seguridad", FYI 36, RFC 2828, mayo de 2000.

7 Agradecimientos

Agradecemos los comentarios constructivos recibidos de Harald Alvestrand, Byron Collie, Barbara Y. Fraser, Gordon Lennox, Andrew Rees, Steve Roming y Floyd corto.

8 Consideraciones de Seguridad

Todo este documento una discusión sobre asuntos de seguridad.

Las direcciones de los autores 9

Dominique Brzezinski
In-Q-Tel
1000 Wilson Blvd., Ste. 2900
Arlington, VA 22209
Estados Unidos

EMail: dbrezinski@In-Q-Tel.org

tom Killalea
Lisi / n na Bro / n
Sea / al A / tha na Muice
Co Mhaigh Eo
IRLANDA

Teléfono: +1 206 266-2196
EMail: tomk@neart.org

10. Declaración de Derechos de autor

Reconocimiento

Financiación de la función del Editor RFC es actualmente el Internet Society.

Nota: la autoria de este anexo, reviste propiedad de la firma NWG (Network Working Group) con patente y autoria de: Dominique Brezinski y Tom Killalea.